الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1525

(2015/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل مواطن الضعف/الحالة

نظام تحديد درجات لمواطن الضعف الشائعة

التوصية ITU-T X.1525

الاتحاد الدولي للاتصالات ITU

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياسات البيومترية عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	**X.1539–X.1520**
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1525

نظام تحديد درجات لمواطن الضعف الشائعة

ملخص

تقدم التوصية ITU-T X.1525 بشأن نظام تحديد الدرجات لمواطن الضعف الشائعة (CWSS) إطاراً مفتوحاً للتعبير عن خصائص وتأثير مواطن الضعف في تكنولوجيا المعلومات والاتصالات (ICT) أثناء تطوير قدرات البرمجيات. والهدف من هذه التوصية تمكين مطوري برمجيات تكنولوجيا المعلومات والاتصالات والمديرين والقائمين على الاختبار وموردي خدمات الأمن ومقدمي الخدمات والمشترين وموردي التطبيقات والباحثين، من التخاطب بلغة مشتركة لتقييم مواطن الضعف في تكنولوجيا المعلومات والاتصالات التي يمكن أن تظهر كثغرات عند استعمال البرمجيات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1525	2015-04-17	17	11.1002/1000/12357

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

يواجه مطور البرمجيات في الغالب مئات أو آلاف من تقارير الخلل الفردية المتعلقة بمواطن الضعف المكتَشفة في شفراتهم. بل إن موطن الضعف البرمجي يمكن أن يؤدي في بعض الأحيان إلى ثغرة قابلة للاستغلال. وبالنظر إلى هذا الحجم الضخم من مواطن الضعف المبلغ عنها يُضطر أصحاب المصلحة في كثير من الأحيان إلى ترتيب المسائل التي ينبغي أن يتحققوا منها ويباشروا بإصلاحها طبقاً للأولوية. وباختصار فإن الناس بحاجة إلى أن تفكر وتتواصل بشأن الأهمية النسبية لمواطن الضعف المختلفة. وهناك طرق متباينة تُستخدم اليوم للتقييم إلا أنها مرتجلة أو غير مناسبة للتطبيق على التقييم الذي ما يزال غير دقيق لأمن البرمجيات. ويوفر نظام تحديد الدرجات لمواطن الضعف الشائعة آلية لترتيب أولويات مواطن الضعف البرمجية بطريقة متسقة، ومرنة، ومفتوحة مع القيام في الوقت ذاته باستيعاب سياق مختلف ميادين الأعمال وأوجه الاستخدام المزمعة للبرمجيات. ويمثل هذا النظام جهداً تعاونياً مجتمعياً يلبي احتياجات أصحاب المصلحة على امتداد الحكومات، والهيئات الأكاديمية، والصناعات.

وعلى مطوري برمجيات تكنولوجيا المعلومات والاتصالات، والمدراء، والقائمين على الاختبار، ومقاولي الأمن وموردي الخدمات، والمشترين، وباعة التطبيقات، والباحثين تحديد وتقدير مواطن الضعف في البرمجيات التي يمكن أن تظهر كثغرات عند استخدامها. كما ينبغي أن يكونوا قادرين على ترتيب أولويات مواطن الضعف هذه واختيار ما يجب إصلاحه منها لأنها تشكل الخطر الأعظم. وحينما تكثر مواطن الضعف التي تحتاج إلى إصلاح، وتحدد درجات كل منها باستخدام مقاييس متفاوتة، يلجأ مختلف أعضاء مجتمع تكنولوجيا المعلومات والاتصالات، والمدراء، والقائمين على الاختبار إلى استعمال منهجياتهم الذاتية لإيجاد وسيلة ما لمقارنة مواطن الضعف المتباينة وتحويلها إلى معلومات صالحة للعمل.

وبالنظر إلى أن نظام تحديد الدرجات لمواطن الضعف الشائعة يوحد النهج المتبع لتشخيص مواطن الضعف فإن بمقدور مستخدميه استحضار سطح الهجمات والمقاييس البيئية لتطبيق المعلومات السياقية بما يعكس بدقة أكبر قدرات البرمجيات بالنظر إلى سياق الأعمال الفريد الذي سيعمل ضمنه وقدرات الأعمال الفريدة التي يُزمع أن يوفرها. ويتيح ذلك لهؤلاء المستخدمين اتخاذ قرارات مستنيرة عند السعي للتخفيف من وطأة المخاطر التي تطرحها مواطن الضعف.

ويستند نظام تحديد الدرجات لمواطن الضعف الشائعة إلى العمل القائم ضمن مجتمع الأمن السيبراني مثل ذلك العدد الضخم من الثغرات المعروفة للعامة والقائمة في العالم الحقيقي المحددة من خلال التوصية [b-ITU-T X.1520] – الثغرات ومواطن التعرض الشائعة ونظام الدرجات المستخدم لمناقشة شدة هذه الثغرات المعروفة للعامة من خلال التوصية [b-ITU-T X.1521] – نظام تحديد درجات الثغرات الشائعة وكذلك قائمة تعداد مواطن الضعف الشائعة بشأن مواطن الضعف في معمارية البرمجيات، أو تصميمها، أو تشفيرها، أو نشرها. ولدى بناء نظام تحديد الدرجات لمواطن الضعف الشائعة جرت مراعاة القدرة على السماح بقيم افتراضية معقولة للمجالات التي قد لا تكون معروفة، مع توفير إمكانية التكييف استناداً إلى سياق الأعمال أو السياق التقني.

وتوصية نظام تحديد الدرجات لمواطن الضعف الشائعة هي واحدة من فئات التوصيات الصادرة عن قطاع تقييس الاتصالات في الاتحاد ويتولاها وسط كبير وقائم وعالمي من المعنيين بالتنمية والمستعملين ممّن يقومون بتدوين وتطوير مواصفة مفتوحة متاحة علناً تقدم إلى قطاع تقيس الاتصالات لكي يعتمدها في إطار اتفاق على أن تُدخل جميع التعديلات أو التحديثات على المواصفة بطريقة تكفل الحفاظ على تحقيق التكافؤ والتوافق الكامل من الناحية التقنية، وأن تُجرى جميع المناقشات حول التعديلات والتحسينات من خلال الاضطلاع بعمليات تخص العالم الأصلي للمستعملين، مع إشارة صريحة إلى الإصدار المحدد المقابل الذي يخضع لرعاية عالم المستعملين. وهكذا فعندما تُعتمد التوصية ITU-T X.1525 اعتماداً أولياً، سيتحقَّق الاحتياط الواجب، مع إعلان بالتكافؤ؛ وعندما يجري سريان التعديلات المدخلة فيما بين أوساط المستعملين، ستتجسّد هذه التعديلات في الوقت المناسب في إصدارات لاحقة من التوصية من خلال التعاون المستمر.

وأُعدت التوصية ITU-T X.1525 – نظام تحديد الدرجات لمواطن الضعف الشائعة بالتعاون مع مؤسسة MITRE، أخذاً في الاعتبار أهمية الحفاظ، قدر الإمكان، على التوافق التقني بين هذه التوصية و"نظام تحديد الدرجات لمواطن الضعف الشائعة"، الإصدار 1.0.1، المؤرخ 5 سبتمبر 2014 [https://cwe.mitre.org/cwss/cwss_v1.0.1.html].

التوصية ITU-T X.1525

نظام تحديد درجات لمواطن الضعف الشائعة

1 مجال التطبيق

تقدم هذه التوصية نهجاً موحداً للتعبير عن خصائص وتأثيرات نقاط الضعف أثناء تطوير قدرات برمجيات تكنولوجيا المعلومات والاتصالات باستخدام سطح هجمات ومقاييس بيئية لتطبيق المعلومات السياقية. ويعكس نظام تحديد الدرجات لمواطن الضعف الشائعة بدقة أكبر الخطر الذي يتعرض له المستخدم من قدرات البرمجيات بالنظر إلى سياق الأعمال الفريد الذي سيعمل ضمنه وقدرات الأعمال الفريدة التي توفرها البرمجيات لهذا المستخدم.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا توجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 النفاذ (access) [b-ITU-T X.1521]: قدرة طرف فاعل على رؤية طرف مفعول به وتعديله والتواصل معه. ويتيح النفاذ تدفق المعلومات بين هذين الطرفين.

2.1.3 التيسر (availability) [b-ITU-T X.1521]: موثوقية الأفراد المخولين ونفاذهم في الوقت المناسب إلى البيانات والموارد.

3.1.3 حالة هجوم (attack instance) [b-ITU-T X.1544]: هجوم محدد بالتفصيل ضد تطبيق أو نظام ويستهدف مواطن التعرض أو الضعف في ذلك النظام.

4.1.3 السرية (confidentiality) [b-ITU-T X.1521]: مبدأ أمني يعمل على ضمان عدم الإفصاح عن معلومات لأطراف غير مخولة.

5.1.3 الحصانة (integrity) [b-ITU-T X.1521]: مبدأ أمني يضمن عدم تعديل المعلومات والأنظمة بسوء نية أو عرضاً.

6.1.3 الخطر (risk) [b-ITU-T X.1521]: التأثير النسبي لموطن ضعف مُستغَل على بيئة المستخدم.

7.1.3 التهديد (threat) [b-ITU-T X.1521]: احتمال أو تواتر وقوع حدث ضار.

8.1.3 الثغرة (vulnerability) [b-ITU-T X.1500]: أي نقطة يمكن استغلالها لانتهاك نظام ما أو المعلومات التي يحتوي عليها.

9.1.3 موطن الضعف (weakness) [b-ITU-T X.1524]: قصور أو نقص في شفرة البرامج أو التصميم أو المعمارية أو الانتشار يمكن أن يتحول في وقت ما إلى ثغرة أو يمكن أن يساهم في إدخال ثغرات أخرى.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.2.3 الصورة المصغرة (vignette): توفر الصورة المصغرة طريقة رسمية قابلة للاقتسام لتحديد بيئة معينة، والدور الذي تضطلع به البرمجيات ضمن هذه البيئة، وأولويات المنظمة فيما يتصل بأمن البرمجيات.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

AI	مرات الاستيقان *(Authentication Instances)*
AL	طبقة الامتياز المكتسب *(Acquired privilege Layer)*
AP	الامتياز المكتسب *(Acquired Privilege)*
AS	شدة الاستيقان *(Authentication Strength)*
ASLR	عشوائية مستوى حيز العناوين *(Address Space Layout Randomization)*
AV	متجه النفاذ *(Access Vector)*
BI	الأثر على الأعمال *(Business Impact)*
BVC	سياق قيمة الأعمال *(Business Value Context)*
CD	قرص مدمج *(Compact Disc)*
CIO	رئيس قسم المعلومات *(Chief Information Officer)*
CSO	رئيس قسم الأمن *(Chief Security Officer)*
CSRF	الطلب المزور العابر للمواقع *(Cross-Site-Request-Forgery)*
CVSS	نظام تحديد الدرجات للثغرات الشائعة *(Common Vulnerability Scoring System)*
CWE	تعداد مواطن الضعف الشائعة *(Common Weakness Enumeration)*
CWRAF	إطار تحليل أخطار مواطن الضعف الشائعة *(Common Weakness Risk Analysis Framework)*
CWSS	نظام تحديد الدرجات لمواطن الضعف الشائعة *(Common Weakness Scoring System)*
DI	احتمال الاكتشاف *(Likelihood of Discovery)*
DNS	نظام أسماء الميادين *(Domain Name System)*
DS	نطاق النشر *(Deployment Scope)*
EC	فعالية الضبط الخارجي *(External Control effectiveness)*
EX	احتمال الاستغلال *(Likelihood of Exploit)*
FC	ثقة الكشف *(Finding Confidence)*
FTP	بروتوكول نقل الملفات *(File Transfer Protocol)*
HTML	لغة وسم النصوص الموسوعية *(Hyper Text Markup Language)*
IC	فعالية الضبط الداخلي *(Internal Control Effectiveness)*
ICT	تكنولوجيا المعلومات والاتصالات *(Information Communication Technology)*
IN	طبقة التفاعل *(level of Interaction)*
IP	بروتوكول الإنترنت *(Internet Protocol)*
NIST	المعهد الوطني للمعايير والتكنولوجيا *(National Institute of Standards and Technology)*
OS	نظام التشغيل *(Operating System)*

OWASP مشروع أمن تطبيقات الإنترنت المفتوحة *(Open Web Application Security Project)*

P الانتشار *(Prevalence)*

PCI DSS معيار أمن بيانات صناعة بطاقات الدفع *(Payment Card Industry Data Security Standard)*

RL طبقة الامتياز المطلوب *(Required Privilege Layer)*

RP الامتياز المطلوب *(Required Privilege)*

SAMATE تقييم مقاييس وأدوات التحقق من البرمجيات *(Software Assurance Metrics And Tool Evaluation)*

SANS إدارة النظام، والمراجعة، والربط الشبكي، والأمن *(SysAdmin, Audit, Networking, and Security)*

SQL لغة الاستعلام البنيوية *(Structured Query Language)*

SSL طبقة المقابس الآمنة *(Secure Sockets Layer)*

TI الأثر التقني *(Technical Impact)*

TLS أمن طبقة النقل *(Transport Layer Security)*

USB الناقل التسلسلي الشامل *(Universal Serial Bus)*

XSS البرمجة العابرة للمواقع *(Cross Site Scripting)*

5 الاصطلاحات

لا توجد.

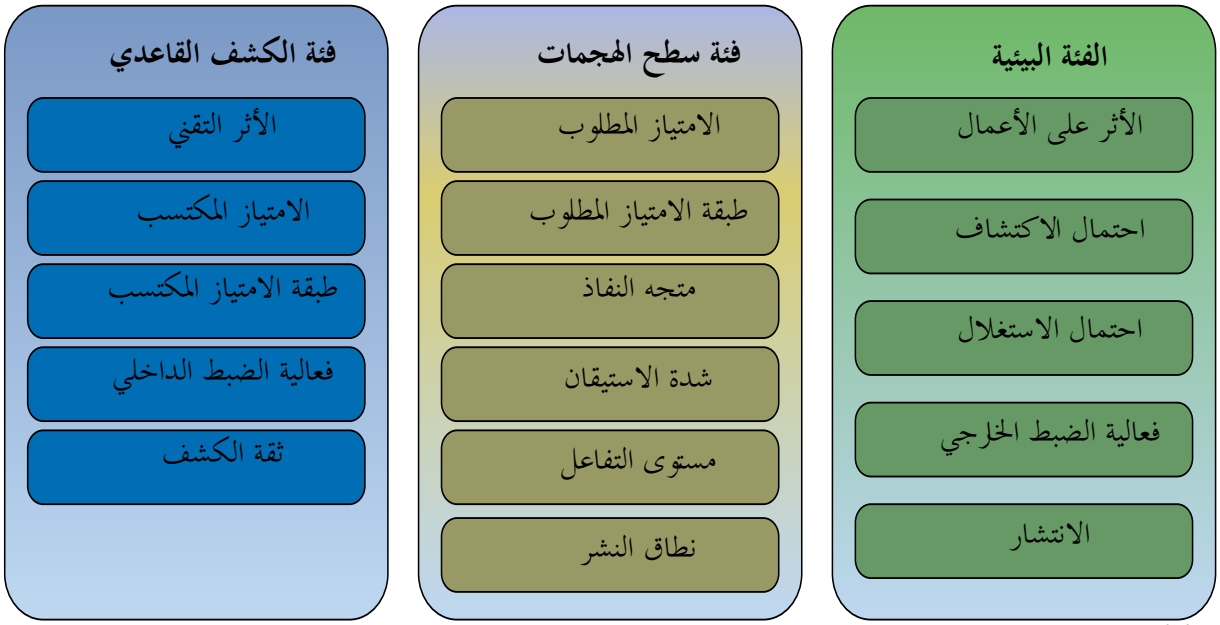
6 استخدام نظام تحديد الدرجات لمواطن الضعف الشائعة

على مطوري برمجيات تكنولوجيا المعلومات والاتصالات، والمدراء، والقائمين على الاختبار، ومقاولي الأمن وموردي الخدمات، والمشترين، وباعة التطبيقات، والباحثين في الوقت الراهن تحديد وتقدير مواطن الضعف في البرمجيات التي يمكن أن تظهر كثغرات عند استخدامها. كما ينبغي أن يكونوا قادرين على ترتيب أولويات مواطن الضعف هذه واختيار ما يجب إصلاحه منها لأنها تشكل الخطر الأعظم. وحينما تكثر مواطن الضعف التي تحتاج إلى إصلاح، وتحدد درجات كل منها باستخدام مقاييس متفاوتة، يلجأ مختلف أعضاء مجتمع تكنولوجيا المعلومات والاتصالات، والمدراء، والقائمين على الاختبار، والمشترين، والمطورين إلى استعمال منهجياتهم الذاتية لإيجاد وسيلة ما لمقارنة مواطن الضعف المتباينة وتحويلها إلى معلومات صالحة للعمل. ونظام تحديد الدرجات لمواطن الضعف هو إطار مفتوح يتناول هذه القضية. وهو يقدم الفوائد التالية:

- القياسات الكمية: يوفر نظام تحديد الدرجات لمواطن الضعف الشائعة قياساً كمياً لمواطن الضعف غير المصححة التي قد تكون قائمة في تطبيق برمجي.
- الإطار المشترك: يوفر نظام تحديد الدرجات لمواطن الضعف الشائعة إطاراً مشتركاً لتحديد أولويات الأخطاء الأمنية ("مواطن الضعف") المكتشفة في التطبيقات البرمجية.
- الترتيب المكيَّف للأولويات: يمكن استخدام نظام تحديد الدرجات لمواطن الضعف الشائعة بالترافق مع إطار تحليل أخطار مواطن الضعف الشائعة "Common Weakness Risk Analysis Framework (CWRAF) [b-CWRAF]" من جانب المستهلكين لتحديد أهم أنماط مواطني الضعف الشائعة في ميادين أعمالهم بغية الاستنارة بذلك فيما يقومون به من أنشطة للحيازة والحماية كجزء واحد من عملية أوسع لتحقيق التثبت من البرمجيات.

1.6 وصف نظام تحديد الدرجات لمواطن الضعف الشائعة

يتوزع نظام تحديد الدرجات لمواطن الضعف الشائعة على ثلاث *فئات للمقاييس* هي: فئة الكشف القاعدي، وفئة سطح الهجمات، والفئة البيئية على النحو الموضح في الشكل 1. وتضم كل فئة مقاييس متعددة، تُعرف أيضاً باسم *العوامل*، تُستخدم في حساب درجات مواطن الضعف وفقاً لنظام تحديد الدرجات لمواطن الضعف الشائعة.



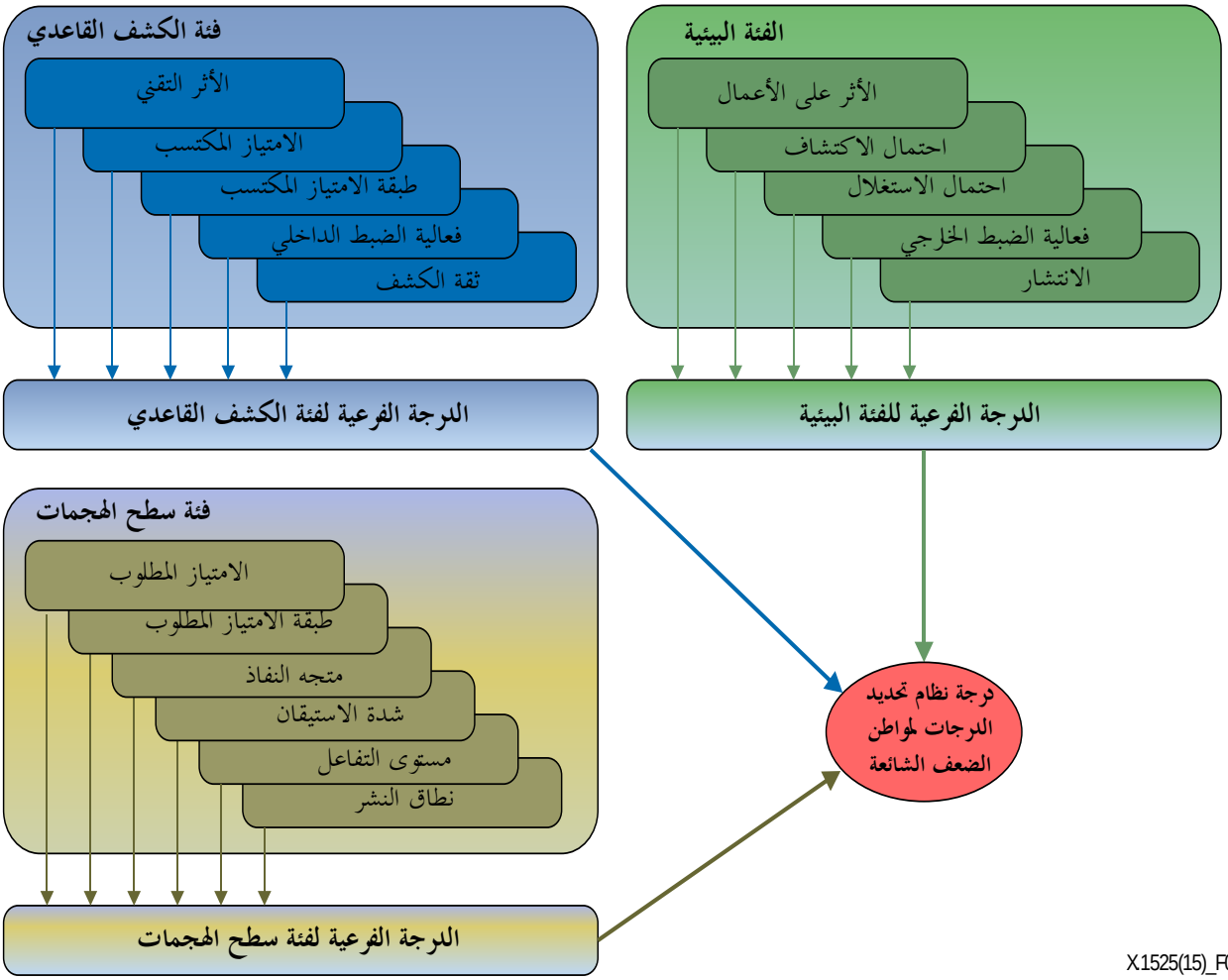
الشكل 1 – فئات مقاييس نظام تحديد الدرجات لمواطن الضعف الشائعة

وتوصف فئات المقاييس على النحو التالي:

- فئة مقاييس الكشف القاعدي: وتستخلص الخطر المتأصل في موطن الضعف، ومدى الثقة في دقة الكشف، وشدة تدابير الرقابة. وتُناقش هذه الفئة في البند 3.7.
- فئة مقاييس سطح الهجمات: الحواجز التي يتعين على المهاجم اختراقها بغية استغلال موطن الضعف. وتُناقش هذه الفئة في البند 4.7.
- فئة المقاييس البيئية: سمات موطن الضعف الخاصة ببيئة معينة أو سياق تشغيلي. وتُناقش هذه الفئة في البند 5.7.

2.6 كيفية عمل نظام تحديد الدرجات لمواطن الضعف الشائعة

يُمنح كل عامل في فئة مقاييس الكشف القاعدي قيمة ما. وتحوَّل هذه القيم إلى أوزان مصاحبة، ويتم حساب الدرجة الفرعية للكشف القاعدي. ويمكن أن تتراوح هذه الدرجة بين 0 و100. وتُطبق الطريقة ذاتها على فئة مقاييس سطح الهجمات وفئة المقاييس البيئية؛ وتتراوح درجاتهما بين 0 و1. وأخيراً تُضرب الدرجات الفرعية ببعضها مما يؤدي إلى إنتاج درجة لنظام تحديد الدرجات لمواطن الضعف الشائعة تتراوح بين 0 و100 على النحو الموضح في الشكل 2.



الشكل 2 – تحديد الدرجات في نظام تحديد الدرجات لمواطن الضعف الشائعة

3.6 تحديد الدرجات في نظام تحديد الدرجات لمواطن الضعف الشائعة

يتعاون مجتمع أصحاب المصلحة مع مؤسسة MITRE لدراسة عدد من الطرق المختلفة لتحديد الدرجات التي قد يتطلب الأمر دعمها ضمن إطار نظام تحديد الدرجات لمواطن الضعف الشائعة. والطرق الأربع الراهنة لتحديد الدرجات هي التالية:

الموجهة تحدد درجات مواطن الضعف الفردية المكتشفة في تصميم أو تنفيذ حزمة برمجية معينة ("مقصودة")، مثل فيض الدارئ في اسم المستخدم في روتين الاستيقان في السطر 1234 من ملف server.c في حزمة مخدم بروتوكول نقل الملفات. وتستخدم الأدوات المؤتمتة والخبراء الاستشاريون لأمن البرمجيات طرقاً موجهة عند تقييم أمن الحزمة البرمجية من حيث مواطن الضعف الكامنة ضمن الحزمة.

العامة تحدد درجات أنواع من مواطن الضعف بغض النظر عن أي حزمة برمجية معينة بغية ترتيب الأولويات فيما بينها (مثل "فيوض الدارئ تتمتع بأولوية أعلى من تسريبات الذاكرة"). ويُستخدم هذا النهج من جانب CWE/SANS Top 25 وOWASP Top Ten، وجهود أخرى مماثلة، وكذلك من قِبل بعض أجهزة مسح الشفرات المؤتمتة. ويمكن أن يكون الفارق شاسعاً بين الدرجات العامة والدرجات الموجهة الناجمة عن التحليل الكامل للوقائع الفردية لنوع موطن الضعف ضمن حزمة برمجية معينة. وعلى سبيل المثال، فإن تدفقات الدارئ تظل مهمة جداً للكثير من المطورين إلا أن الاختلالات الفردية لتدفقات الدارئ قد تعتبر أقل أهمية إذا تعذر تحفيزها من جانب مهاجم وخُفِّض أثرها بفعل آليات الحماية على مستوى نظام التشغيل مثل عشوائية مستوى حيز العناوين.

المعدلة حسب السياق	تُعدِّل الدرجات وفقاً لاحتياجات السياق التحليلي المعين الذي قد يدمج أولويات الأعمال/المهام، وبيئات التهديد، ومدى تحمل المخاطر، وما إلى ذلك. وتُستخلص هذه الاحتياجات باستخدام صور مصغرة تربط السمات المتأصلة لمواطن الضعف مع اعتبارات الأعمال الرفيعة المستوى. ويمكن استخدام هذه الطريقة في التحديد الموجه والعام للدرجات على حد سواء.
التجميعية	تجمع بين نتائج درجات مواطن الضعف المتعددة وذات المستوى المنخفض لإنتاج درجة كلية منفردة (أو "علامة"). وفي حين أن التجميع قد يكون أيسر تطبيقاً على الطريقة الموجهة فإن بالمستطاع استعماله أيضاً في التحديد العام للدرجات، على نحو ما حدث في قائمة CWE/SANS Top 25 لعام 2010.

وتجدر الإشارة إلى أن التركيز الراهن ينصب في معظم المناقشات المتعلقة بنظام تحديد الدرجات لمواطن الضعف الشائعة على الطريقة الموجهة لتحديد الدرجات وعلى إطار تحديد للدرجات معدل حسب السياق. وستلي ذلك طرق للتحديد التجميعي للدرجات. ويجري تطوير التحديد العام للدرجات بصورة مستقلة، وذلك أساساً كجزء من قائمة Top 25 لعام 2011 وإطار تحليل أخطار مواطن الضعف الشائعة.

ويمكن حساب درجات نظام تحديد الدرجات لمواطن الضعف الشائعة آلياً، وذلك مثلاً بأداة لتحليل التشفير، كما يمكن حسابها يدوياً من جانب خبير استشاري لأمن البرمجيات أو مطور للبرمجيات. وبما أن من المستبعد أن يمتلك التحليل المؤتمت بعض المعلومات المتاحة، مثل بيئة تشغيل التطبيق، فقد يكون بالمستطاع تحديد درجات نظام تحديد الدرجات لمواطن الضعف الشائعة على جولات متعددة: حيث تقوم أداة أولاً بالحساب الآلي لدرجات نظام تحديد الدرجات لمواطن الضعف الشائعة، ثم يضيف المحلل البشري يدوياً تفاصيل إضافية ويعيد حساب الدرجات.

4.6 مستخدمو نظام تحديد الدرجات لمواطن الضعف الشائعة

تحقيقاً لأقصى درجات الفعالية فإن نظام تحديد الدرجات لمواطن الضعف الشائعة يدعم سيناريوهات مختلفة للاستخدام من جانب أصحاب المصلحة المتباينين المهتمين جميعاً بتوافر نظام متسق لتحديد الدرجات لوضع ترتيب من حيث الأولوية لمواطن ضعف البرمجيات التي يمكن أن تجلب أخطاراً على المنتجات، والنظم، والشبكات، والخدمات. وترد أدناه بعض الأمثلة على أصحاب المصلحة الرئيسيين:

- مطورو البرمجيات: يعمل المطورون غالباً في ظل أطر زمنية محدودة وذلك بفعل دورات الإصدار وقلة الموارد. ونتيجة لذلك فإنهم يعجزون عن التحقق من كل موطن ضعف مبلغ عنه وتصحيحه. وقد يختارون التركيز على أسوأ المشكلات وعلى الأسهل على الحل. وفي حالة الكشف الآلي عن مواطن الضعف فقد يفضلون التركيز على الاكتشافات التي تقل احتمالات أن تكون إيجابية زائفة.
- مدراء تطوير البرمجيات: يستحدث مدراء تطوير البرمجيات استراتيجيات لترتيب الأولويات بشأن إزالة أنواع كاملة من مواطن الضعف من قاعدة التشفير الكاملة، أو على الأقل ذلك الجزء الذي يعتبر أكثر تعرضاً للخطر، ومن المحتمل أن يتم ذلك بوضع قوائم مخصصة بالأخطار الكبرى. وينبغي أن يتفهم هؤلاء المدراء الآثار الأمنية لإدماج برمجيات طرف ثالث قد تحتوي على مواطن ضعفه الخاصة. وقد يحتاجون إلى دعم متطلبات أمنية متميزة وتحديد الأولويات لكل خط إنتاجي.
- حائزو البرمجيات: يرغب الزبائن، بما في ذلك موظفو توفير الحيازة، في الحصول على برمجيات طرف ثالث بمستوى معقول من الضمان بأن مورِّد البرمجيات قد اعتمد الاحتياط الواجب في إزالة أو تفادي مواطن الضعف الأكثر أهمية بالنسبة لأعمال الحائز ومهامه. ويشمل أصحاب المصلحة المعنيون كلاً من رؤساء أقسام المعلومات، ورؤساء أقسام الأمن، ومديري النظم، والمستخدمين النهائيين للبرمجيات.
- مدراء أمن الشركات: يسعى مدراء أمن الشركات إل التقليل من الأخطار ضمن شركاتهم وذلك فيما يتعلق بالثغرات المعروفة في منتجات الطرف الثالث، وكذلك الثغرات (أو مواطن الضعف) في برمجياتهم الداخلية الذاتية. وقد يرغبون في استخدم آلية لتحديد الدرجات يمكن أن تتكامل مع العمليات الأخرى لإدارة الأمن، مثل جمع نتائج مسح ثغرات الطرف الثالث (المتعلقة بالثغرات المعروفة للطرف الثالث) مع تحليل التطبيقات المخصص (للبرمجيات الداخلية) للمساعدة في تقدير الخطر الكلي لأصل من الأصول.

- الباعة والخبراء الاستشاريون المعنيون بتحليل التشفير: غالباً ما يمتلك الباعة والخبراء تقنيات خاصة بهم لتحديد الدرجات، ولكنهم يرغبون بتوفير آلية متسقة خضعت لتمحيص ذوي الاختصاص للزبائن المختلفين.
- مقيمو قدرات تحليل التشفير: يقوم المقيمون بتحليل وقياس قدرات تحليل التشفير (مثل NIST SAMATE). وبمقدورهم استخدام آلية متسقة لتحديد درجات مواطن الضعف لدعم عمليات أخذ عينات الكشوف المبلغ عنها، وكذلك لفهم شدة هذه الكشوف دون الاعتماد على طرق مرتجلة لتحديد الدرجات قد تتباين بشكل شاسع من حيث الأدوات/ التقنيات.
- أصحاب المصلحة الآخرون: يمكن أن يشمل أصحاب المصلحة الآخرون الباحثين المعنيين بالثغرات، ومناصري النشر المضمون، والمحللين المستندين إلى الامتثال (مثل معيار أمن بيانات قطاع بطاقات الدفع).

واعتباراً من يونيو 2014 (حينما دخلت النسخة 0.8 من نظام تحديد الدرجات لمواطن الضعف الشائعة حيز التشغيل) كانت هناك عمليات تنفيذ متعددة في العالم الواقعي لهذا النظام. أما المستخدمون الرئيسيون للنظام فكانوا باعة تحليلات التشفير وخبراء أمن البرمجيات.

7 فئات المقاييس

1.7 عوامل فئات المقاييس

يتضمن نظام تحديد الدرجات لمواطن الضعف الشائعة العوامل التالية التي تم توزيعها على أساس فئة مقاييسها على النحو الموضح في الجدول 1 أدناه. ويرد وصف مفصل لكل عامل في البنود اللاحقة.

الجدول 1 – عوامل فئات المقاييس

الفئة	الاسم	الملخص
الكشف القاعدي	الأثر التقني (TI)	يمكن أن يُحدث موطن الضعف النتيجة المحتملة بافتراض أن بالمستطاع النجاح في الوصول إلى هذا الموطن واستغلاله.
	الامتياز المكتسب (AP)	نوع الامتياز الذي يكتسبه المهاجم الذي ينجح في استغلال موطن الضعف.
	طبقة الامتياز المكتسب (AL)	الطبقة التشغيلية التي يُحرز فيها المهاجم امتيازات عبر نجاحه في استغلال موطن الضعف.
	فعالية الضبط الداخلي (IC)	قدرة تدبير الضبط على جعل موطن الضعف غير قابل للاستغلال من جانب المهاجم.
	ثقة الكشف (FC)	الثقة بأن المسألة المبلغ عنها هي موطن ضعف يمكن أن يستغله المهاجم.
سطح الهجمات	الامتياز المطلوب (RP)	نوع الامتيازات التي يجب أن يمتلكها المهاجم بالفعل للوصول إلى الشفرة/الوظيفة المحتوية على موطن الضعف.
	طبقة الامتياز المطلوب (RL)	الطبقة التشغيلية التي ينبغي أن يمتلك فيها المهاجم امتيازات لمحاولة الهجوم على موطن الضعف.
	متجه النفاذ (AV)	القناة التي يجب أن يتواصل فيها المهاجم للوصول إلى الشفرة أو الوظيفة المحتوية على موطن الضعف.
	شدة الاستيقان (AS)	شدة إجراء الاستيقان الذي يحمي الشفرة/الوظيفة المحتوية على موطن الضعف.
	مستوى التفاعل (IN)	التدابير المطلوبة من الضحية (الضحايا) البشرية للتمكين من تنفيذ هجوم ناجح.
	نطاق النشر (SC)	ما إذا كان موطن الضعف موجوداً في كل حالات البرمجية القابلة للنشر، أو ما إذا كان مقتصراً على مجموعة فرعية من المنصات و/أو التشكيلات.

الفئة	الاسم	الملخص
الفئة البيئية	الأثر على الأعمال (BI)	الأثر المحتمل على الأعمال أو المهمة في حال النجاح في استغلال موطن الضعف.
	احتمال الاكتشاف (DI)	احتمال تمكن المهاجم من اكتشاف موطن الضعف.
	احتمال الاستغلال (EX)	احتمال تمكن مهاجم متمتع بالامتيازات/الاستيقان/النفاذ من أن ينجح في استغلال موطن الضعف عند اكتشافه.
	فعالية الضبط الخارجي (EC)	قدرة الضوابط أو تدابير التخفيف خارج البرمجية التي قد تزيد من الصعوبات التي يواجهها المهاجم في الوصول إلى موطن الضعف و/أو تحفيزه.
	الانتشار (P)	وتيرة ظهور هذا النمط من موطن الضعف في البرمجية.

2.7 قيم عدم التأكد والمرونة

يمكن استخدام نظام تحديد الدرجات لمواطن الضعف الشائعة في الحالات التي تتوافر فيها معلومات قليلة فحسب في بادئ الأمر ثم تتحسن نوعية هذه المعلومات مع مضي الوقت. ومن المتوقع في العديد من حالات الاستخدام أن تتغير درجة النظام المتعلقة بكشف موطن ضعف فردي كثيراً مع اكتشاف المزيد من المعلومات. وقد تقوم كيانات مختلفة بتقييم عوامل منفصلة في نقاط زمنية متباينة.

وعلى هذا فإن لكل عامل من عوامل نظام تحديد الدرجات لمواطن الضعف الشائعة فعلياً سمات "بيئية" أو "مؤقتة"، ولذلك فإن من غير المفيد على وجه الخصوص اعتماد الأنماط ذاتها لفئات المقاييس على نحو ما هو متبع في نظام تحديد درجات الثغرات الشائعة.

وتشترك معظم العوامل بالقيم الأربع المعروضة في الجدول 2 أدناه.

الجدول 2 – قيم عوامل عدم التأكد والمرونة

القيمة	الاستخدام
مجهولة	لا يمتلك الكيان القائم بحساب الدرجات معلومات كافية لتوفير قيمة للعامل. وقد يكون ذلك إشارة إلى ضرورة إجراء المزيد من التحقيقات. وعلى سبيل المثال، فإن جهازاً أوتوماتياً لمسح الشفرة قد يكون قادراً على العثور على بعض أنواع مواطن الضعف ولكنه عاجز عن الكشف عما إذا كانت هناك أية آليات قائمة للاستيقان. ويؤكد استخدام "مجهولة" أن الدرجة غير مستكملة أو مقدرة وأن الحاجة قد تدعو إلى مزيد من التحليل. وييسر ذلك نمذجة المعلومات غير المستكملة، وممارسة سياق قيمة الأعمال التأثير على الدرجات النهائية التي تم منحها بالاستناد إلى المعلومات غير المستكملة. ويبلغ الوزن الترجيحي لهذه القيمة 5,0 لكل العوامل، وهو ما يسفر عموماً عن درجة أدنى؛ وستؤدي إضافة المعلومات الجديدة (أي تغيير صفة بعض العوامل من "مجهولة" إلى قيمة أخرى) عندها إلى تعديل الدرجة صعوداً أو هبوطاً تبعاً للمعلومات الجديدة.
غير منطبقة	يتم تجاهل العامل صراحةً في حساب الدرجات. ويتيح ذلك فعلاً لقيمة سياق الأعمال أن تفرض ما إذا كان العامل ذا صلة بالدرجة النهائية. وعلى سبيل المثال، فإن طريقة تتركز على الزبون من طرق تحديد الدرجات في نظام تحديد الدرجات لمواطن الضعف الشائعة قد تتجاهل جهود المعالجة، وقد تتطلب بيئة الضمان العالي التحقيق في كل الكشوف المبلغ عنها، حتى لو انخفضت الثقة في مدى دقتها. وبالنسبة لمجموعة من الكشوف المتعلقة بمواطن الضعف فإن من المتوقع أن يكون لكل الكشوف قيمة "غير منطبقة" ذاتها فيما يتعلق بالعامل الجاري تجاهله.
محددة كمياً	يمكن تحديد الوزن الترجيحي للعامل باستخدام نطاق متواصل محدد كمياً من 0,0 إلى 0,1 عوضاً عن المجموعة المحددة من القيم المنفصلة للعامل. وليست كل العوامل قابلة للتحديد الكمي على هذا النحو، ولكن ذلك يسمح بمزيد من التكييف للمقياس.
افتراضية	يمكن تحديد الوزن الترجيحي للعامل كقيمة افتراضية. ويتيح توصيف العامل بأنه افتراضي إجراء التحقيقات واحتمال التعديل في وقت لاحق.

3.7 فئة مقاييس الكشف القاعدي

تتألف فئة مقاييس الكشف القاعدي من العوامل التالية:

- الأثر التقني (TI)

- الامتياز المكتسب (AP)
- طبقة الامتياز المكتسب (AL)
- فعالية الضبط الداخلي (IC)
- ثقة الكشف (FC)

وتمنح توليفة القيم من الأثر التقني، والامتياز المكتسب، وطبقة الامتياز المكتسب، وفعالية الضبط الداخلي، وثقة الكشف المستخدم بعض القوة التعبيرية. فعلي سبيل المثال، فإن المستخدم يمكن أن يصف الأثر التقني بـ "العالي" مع امتياز "مدير" عند طبقة "التطبيق".

1.3.7 الأثر التقني (TI)

إن الأثر التقني هو النتيجة المحتملة التي يمكن أن يُحدثها موطن الضعف بافتراض أن بالمستطاع النجاح في الوصول إلى هذا الموطن واستغلاله. ويتم الإعراب عن ذلك بتعابير أكثر دقة من تعابير السرية، والحصانة، والتيسر.

وينبغي تقييم الأثر التقني بالنسبة للامتياز المكتسب (AP) وطبقة الامتياز المكتسب (AL).

الجدول 3 – الأوزان الترجيحية للأثر التقني

القيمة	الرمز	الوزن الترجيحي	الوصف
حرجة	C	1,0	سيطرة كاملة على البرمجية الخاضعة للتحليل إلى درجة تَعذُّر القيام بالعمليات.
عالية	H	0,9	سيطرة واسعة على البرمجية الخاضعة للتحليل، أو أن بالمستطاع النفاذ إلى المعلومات البالغة الأهمية.
متوسطة	M	0,6	سيطرة معتدلة على البرمجية الخاضعة للتحليل، أو أن بالمستطاع النفاذ إلى المعلومات ذات الأهمية المعتدلة.
منخفضة	L	0,3	سيطرة دنيا على البرمجية الخاضعة للتحليل، أو أن بالمستطاع النفاذ فحسب إلى المعلومات غير الهامة نسبياً.
لا شيء	N	0,0	ليس هناك من أثر تقني على البرمجية الخاضعة للتحليل على الإطلاق. وبعبارة أخرى فإن ذلك لا يقود إلى ثغرة.
افتراضية	D	0,6	إن الوزن الترجيحي الافتراضي هو متوسط أوزان القيم الحرجة، والعالية، والمتوسطة، والمنخفضة، وقيمة لا شيء.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية؛ وقد يرغب المستخدم في التحقيق في كل كشف مثير للاهتمام عن مواطن الضعف بغض النظر عن مدى الثقة.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

وإذا لم تكن هذه المجموعة من القيم دقيقة بما فيه الكفاية فإن بمقدور مستخدمي نظام تحديد الدرجات لمواطن الضعف الشائعة استعمال طرقهم الذاتية المحددة كمياً لاستخلاص الدرجات الفرعية. وتشمل إحدى هذه الطرق استخدام إطار تحليل أخطار مواطن الضعف الشائعة [b-CWRAF] (CWRAF) لتحديد صورة مصغرة وبطاقة درجات للأثر التقني. ويُحسب الوزن الترجيحي للأثر باستخدام تصنيفات أهمية خاصة بالصورة المصغرة لمختلف الآثار التقنية التي قد تنشأ عن استغلال موطن الضعف، مثل تعديل البيانات الحساسة، واكتساب الامتيازات، واستهلاك الموارد، وما إلى ذلك.

2.3.7 الامتياز المكتسب (AP)

يحدد الامتياز المكتسب نوع الامتيازات التي يكتسبها المهاجم الذي ينجح في استغلال موطن الضعف.

ويشار إلى أن القيم هي ذاتها القيم المتعلقة بالامتياز المطلوب، إلا أن الأوزان الترجيحية متباينة.

وفي بعض الحالات قد تكون قيمة الامتيازات المكتسبة هي ذاتها قيمة الامتيازات المطلوبة وهي ما يدل على ما يلي: (1) تصاعد الامتيازات "الأفقي" (من مستخدم محروم من الامتيازات إلى آخر، أو (2) تصاعد الامتيازات ضمن جهاز افتراضي مثل بروتوكول لنقل الملفات الذي لا يتسنى النفاذ إلى سطحه البيني إلا للمستخدم.

الجدول 4 – الأوزان الترجيحية للامتياز المكتسب

القيمة	الرمز (ملاحظة)	الوزن الترجيحي	الوصف
مدير	A	1,0	يتمكن المهاجم من النفاذ إلى الكيان بامتيازات مدير، أو جذر، أو نظام، أو ما يكافئ ذلك وهو ما يعني السيطرة الكاملة على البرمجية الخاضعة للتحليل؛ أو أن بمقدور المهاجم أن يزيد من امتيازاته الذاتية (الأدنى) لتصبح امتيازات مدير.
مستخدم ذو امتيازات جزئية	P	0,9	يتمكن المهاجم من النفاذ إلى الكيان ببعض الامتيازات الخاصة، ولكنها ليست كافية لتعادل امتيازات المدير؛ أو أن بمقدور المهاجم أن يزيد من امتيازاته الذاتية (الأدنى) إلى مستوى مستخدم ذي امتيازات جزئية. وعلى سبيل المثال، فإن المستخدم قد يتمتع بامتيازات استخلاص نسخ احتياطية، ولكن دون أن يستطيع تعديل تشكيل البرمجية أو تحيينها.
مستخدم عادي	RU	0,7	يتمكن المهاجم من النفاذ إلى الكيان كمستخدم عادي دون أي امتيازات خاصة؛ أو أن بمقدور المهاجم أن يزيد من امتيازاته الذاتية إلى مستوى مستخدم عادي.
محدودة/ضيف	L	0,6	يتمكن المهاجم من النفاذ إلى الكيان بامتيازات محدودة أو امتيازات "ضيف"؛ أو أن بمقدور المهاجم أن يزيد من امتيازاته الذاتية (الأدنى) إلى مستوى ضيف. ملاحظة: لا تشير هذه القيمة إلى مفهوم "نظام التشغيل الخاص بالضيوف" المتعلق بالمستضيفين الافتراضيين.
لا شيء	N	0,1	لا يستطيع المهاجم النفاذ إلى أي امتيازات تزيد عما هو متاح له بالفعل. (تجدر الإشارة إلى أن هذه القيمة يمكن أن تكون مفيدة في الظروف المحدودة التي يستطيع فيها المهاجم الإفلات إلى جهاز افتراضي أو بيئة تقييدية أخرى ولكنه يظل عاجزاً عن كسب امتيازات إضافية أو التمكن من النفاذ مثل المستخدمين الآخرين).
افتراضية	D	0,7	متوسط الأوزان الترجيحية لقيم لا شيء، وضيف، ومستخدم عادي، ومستخدم ذي امتيازات جزئية، ومدير.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية ترغب في إنفاذ صارم لفصل الامتيازات حتى بين المستخدمين ذوي الامتيازات بالفعل.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. ويشار إلى أن القيم المحددة كمياً مدعومة من أجل الاكتمال؛ ولكن بما أن الامتيازات والمستخدمين يشكلان كيانات منفصلة فقد تكون هناك حالات محدودة فحسب يكون فيها النموذج المحدد كمياً مفيداً.
ملاحظة – تسهيلاً للتذكر فإن القيم الأساسية لهذا العامل تُختصر بكلمة "RUNLAP" التي تمثل الأحرف الأولى من تسميات هذه القيم باللغة الإنكليزية (Regular User, None, Limited, Admin, Partially-Privileged).			

3.3.7 طبقة الامتياز المكتسب (AL)

تحدد طبقة الامتياز المكتسب الطبقة التشغيلية التي يُحرز فيها المهاجم امتيازات عبر نجاحه في استغلال موطن الضعف.

الجدول 5 – الأوزان الترجيحية لطبقة الامتياز المكتسب

القيمة	الرمز (ملاحظة)	الوزن الترجيحي	الوصف
التطبيق	A	1,0	يتطلب المهاجم امتيازات مدعومة ضمن البرمجية قيد التحليل ذاتها. (إذا كانت البرمجية قيد التحليل جزءاً أساسياً من النظام الأساسي، مثل نواة نظام التشغيل فقد تكون قيمة النظام عندها مناسبة أكثر).
النظام	S	0,9	يتطلب المهاجم امتيازات إلى النظام الأساسي أو المستضيف المادي المستخدم لتشغيل البرمجية قيد التحليل.
الشبكة	N	0,7	يتطلب المهاجم امتيازات للنفاذ إلى الشبكة.
البنية التحتية للشركة	E	1,0	يتطلب المهاجم امتيازات إلى قطعة بالغة الأهمية من البنية التحتية للشركة، مثل المسيِّر، والبدالة، ونظام أسماء الميادين، وجدار الحماية، ومخدّم الهوية، وما إلى ذلك.
افتراضية	D	0,9	متوسط الأوزان الترجيحية للتطبيق، والنظام، والشبكة، والبنية التحتية للشركة.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية ترغب في إنفاذ صارم لفصل الامتيازات حتى بين المستخدمين ذوي الامتيازات بالفعل.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. ويشار إلى أن القيم المحددة كمياً مدعومة من أجل الاكتمال؛ ولكن بما أن الامتيازات والمستخدمين يشكلان كيانات منفصلة فقد تكون هناك حالات محدودة فحسب يكون فيها النموذج المحدد كمياً مفيداً.
ملاحظة – تسهيلاً للتذكر فإن القيم الأساسية لهذا العامل تُختصر بكلمة "SANE" التي تمثل الأحرف الأولى من تسميات هذه القيم باللغة الإنكليزية (System, Application, Network, Enterprise Infrastructure).			

4.3.7 فعالية الضبط الداخلي (IC)

إن الضبط الداخلي هو تدبير ضبط، أو آلية حماية، أو تدبير للتخفيف تم إدماجه بالبرمجية بصورة صريحة (سواء من خلال المعمارية، أو التصميم، أو التنفيذ). وتقيس فعالية الضبط الداخلي قدرة تدبير الضبط على جعل موطن الضعف غير قابل للاستغلال من جانب المهاجم. وعلى سبيل المثال، فإن روتين التحقق من صحة المدخلات الذي ينص على أن يكون طول المدخل 15 حرفاً كحد أقصى قد يكون فعالاً بشكل معتدل إزاء هجمات كتابة البيانات عبر المواقع (XSS) من خلال الحد من حجم الهجوم من هذا النوع الذي يمكن القيام به.

وحينما تكون هناك ضوابط داخلية متعددة، أو مسارات تشفير متعددة، التي يمكن أن تصل إلى موطن الضعف ذاته فعندها تطبق التوجيهات التالية:

- يتم بالنسبة لكل مسار تشفير تحليل الضبط الداخلي القائم على طول هذا المسار، واختيار القيمة مع أدنى وزن ترجيحي (أي الضبط الداخلي الأقوى على مسار التشفير). ويُطلق على ذلك اسم قيمة مسار التشفير.
- تُجمع كل قيم مسارات التشفير.
- تُنتقى قيمة مسار التشفير ذات الوزن الترجيحي الأعلى (أي ذات الضبط الأضعف).

وتُقيِّم هذه الطريقة كل مسار للتشفير من حيث الضبط الأقوى له (حيث إن على المهاجم الالتفاف على هذا الضابط)، ثم تختار مسار التشفير الأضعف (أي الطريق الأسهل بالنسبة للمهاجم).

الجدول 6 – الأوزان الترجيحية لفعالية الضبط الداخلي

القيمة	الرمز	الوزن الترجيحي	الوصف
لا شيء	N	1,0	ليس هناك من ضوابط.
محدودة	L	0,9	هناك طرق ساذجة أو قيود عرضية قد تمنع مهاجماً عابراً من استغلال المسألة.
معتدلة	M	0,7	تُستخدم آلية الحماية بشكل عام غير أنها ذات قيود معروفة قد يستطيع المهاجم العارف الالتفاف عليها ببعض الجهد. وعلى سبيل المثال، فإن بالمستطاع الالتفاف على تشفير كيان لغة وسم النصوص الموسوعية لمنع هجمات كتابة البيانات عبر المواقع عند وضع الناتج في سياق آخر مثل وريقات الأسلوب المتعاقبة أو سمة العلامة التعريفية للغة وسم النصوص الموسوعية.
غير مباشرة (دفاع في العمق)	I	0,5	لا يوفر الضابط الحماية من استغلال موطن الضعف تحديداً، ولكنه يقلل بصورة غير مباشرة من الأثر عند شن هجوم ناجح. أو أنه يجعل من الصعب إرساء استغلال وظيفي. وعلى سبيل المثال، فإن إجراء التحقق من الصحة يمكن أن يحد بشكل غير مباشر من حجم المدخل، مما قد يزيد من الصعوبة التي تواجه المهاجم في إنشاء حمولة لهجمة من هجمات البرمجة العابرة للمواقع أو هجمة حقن للغة الاستعلام البنيوية.
أفضل المتوافر	B	0,3	يتَّبع الضابط الممارسات الجارية المثلى، ولو أنه قد يتسم ببعض القيود التي يمكن لمهاجم ماهر ومصمم التغلب عليها، وهو ما قد يتطلب وجود مواطن ضعف أخرى. وعلى سبيل المثال، تعتبر طريقة التقديم المزدوج للحماية من الطلب المزور العابر للمواقع من أقوى الطرق المتاحة، ولكن بالمستطاع التغلب عليها بالترافق مع سلوكيات بعض الوظائف القادرة على قراءة الرأسية الأولية لبروتوكول نقل النصوص التشعبية.
كاملة	C	0,0	يتسم الضابط بفعالية كاملة إزاء موطن الضعف، أي أنه ليس هناك من خلل أو ثغرة، ولا عواقب وخيمة لاستغلال المسألة. وعلى سبيل المثال، فإن عملية نسخة الدارئ التي تكفل أن الدارئ المقصود هو أكبر على الدوام من المصدر (بالإضافة إلى أي توسع غير مباشر لحجم المصدر الأصلي) لن تؤدي إلى أي فيض.
افتراضية	D	0,6	متوسط الأوزان الترجيحية لقيم كاملة، وأفضل المتوافر، وغير المباشرة، والمعتدلة، والمحدودة، ولا شيء.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

5.3.7 ثقة الكشف (FC)

ثقة الكشف هي الثقة بأن المسألة المبلغ عنها هي:

1 موطن ضعف،

2 يمكن أن يحفزها أو يستغلها المهاجم.

الجدول 7 – الأوزان الترجيحية لثقة الكشف

القيمة	الرمز	الوزن الترجيحي	الوصف
حقيقية مثبتة	T	1,0	يمكن للمهاجم الوصول إلى موطن الضعف.
حقيقية مثبتة محلياً	LT	0,8	ينشأ موطن الضعف ضمن وظيفة منفردة أو مكوّن منفرد يعتمدان في تصميمهما على استدعاء آمن للوظيفة، غير أن قدرة المهاجم على الوصول إلى هذه الوظيفة غير معروفة أو غير حاضرة. وعلى سبيل المثال، فإن وظيفة المرافق العمومية قد تنشئ استفساراً لقواعد البيانات دون تشفير مدخلاته، ولكن إذا ما كانت تُستدعى بسلاسل ثابتة فحسب فإن الكشف يعتبر حقيقياً محلياً.
زائفة مثبتة	F	0,0	إن الكشف خاطئ (أي أن الكشف زائف موجب وليس هناك من موطن ضعف) و/أو ليس هناك من دور محتمل للمهاجم.
افتراضية	D	0,8	متوسط الأوزان الترجيحية للحقيقية المثبتة، والحقيقية المثبتة محلياً، والزائفة المثبتة.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية؛ وقد يرغب المستخدم في التحقيق في كل كشف مثير للاهتمام عن مواطن الضعف بغض النظر عن مدى الثقة.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. وتتمتع بعض أدوات تحليل التشفير بمقاييس محكمة لمدى دقة بعض أنماط الكشف المحددة.

4.7 فئة مقاييس سطح الهجمات

تتألف فئة مقاييس سطح الهجمات من العوامل التالية:

- الامتياز المطلوب (RP)
- طبقة الامتياز المطلوب (RL)
- متجه النفاذ (AV)
- شدة الاستيقان (AS)
- مستوى التفاعل (IN)
- نطاق النشر (SC).

1.4.7 الامتياز المطلوب (RP)

يحدد الامتياز المطلوب نوع الامتيازات التي يجب أن يمتلكها المهاجم بالفعل للوصول إلى الشفرة/الوظيفة المحتوية على موطن الضعف.

الجدول 8 – الأوزان الترجيحية للامتياز المطلوب

القيمة	الرمز (ملاحظة)	الوزن الترجيحي	الوصف
لا شيء	N	1,0	ليست هناك من امتيازات مطلوبة. وعلى سبيل المثال، فإن محرك بحث شبكي قد لا يحتاج إلى أي امتيازات لأي كيان لإدخال مصطلح بحث ومعاينة النتائج.
محدودة/ضيف	L	0,9	يتمتع الكيان بامتيازات محدودة أو امتيازات "ضيف" وهو ما يمكن أن يحد كثيراً من الأنشطة؛ وقد يكون الكيان قادراً على تسجيل أو إنشاء حساب جديد دون أي متطلبات خاصة أو إثبات للهوية. وعلى سبيل المثال، فإن مدونة شبكية قد تسمح للمشاركين بإنشاء اسم للمستخدم وتقديم عنوان بريدي إلكتروني صحيح قبل إدخال التعليقات. ملاحظة: لا تشير هذه القيمة إلى مفهوم "نظام التشغيل الخاص بالضيوف" المتعلق بالمستضيفين الافتراضيين.
مستخدم عادي	RU	0,7	إن الكيان هو مستخدم عادي لا يتمتع بأي امتيازات خاصة.
مستخدم ذو امتيازات جزئية	P	0,6	إن الكيان هو مستخدم صالح ببعض الامتيازات الخاصة، ولكنها ليست كافية لتعادل امتيازات المدير. وعلى سبيل المثال، فإن المستخدم قد يتمتع بامتيازات استخلاص نسخ احتياطية، ولكن دون أن يستطيع تعديل تشكيل البرمجية أو تحيينها.
مدير	A	0,1	للكيان امتيازات مدير، أو جذر، أو نظام، أو ما يكافئ ذلك وهو ما يعني السيطرة الكاملة على البرمجية أو نظام التشغيل الأساسي.
افتراضية	D	0,7	متوسط الأوزان الترجيحية لقيم لا شيء، ومحدودة، ومستخدم عادي، ومستخدم ذي امتيازات جزئية ومدير.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية ترغب في إنفاذ صارم لفصل الامتيازات حتى بين المستخدمين ذوي الامتيازات بالفعل.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. ويشار إلى أن القيم المحددة كمياً مدعومة من أجل الاكتمال؛ ولكن بما أن الامتيازات والمستخدمين يشكلان كيانات منفصلة فقد تكون هناك حالات محدودة فحسب يكون فيها النموذج المحدد كمياً مفيداً.
ملاحظة – تسهيلاً للتذكر فإن القيم الأساسية لهذا العامل تُختصر بكلمة "RUNLAP" التي تمثل الأحرف الأولى من تسميات هذه القيم باللغة الإنكليزية (Regular User, None, Limited, Admin, Partially-Privileged).			

2.4.7 طبقة الامتياز المطلوب (RL)

تحدد طبقة الامتياز المطلوب الطبقة التشغيلية التي ينبغي أن يمتلك فيها المهاجم امتيازات لمحاولة الهجوم على موطن الضعف.

الجدول 9 – الأوزان الترجيحية لطبقة الامتياز المطلوب

القيمة	الرمز (ملاحظة)	الوزن الترجيحي	الوصف
التطبيق	A	1,0	يجب أن يتمتع المهاجم بامتيازات مدعومة ضمن البرمجية قيد التحليل ذاتها. (إذا كانت البرمجية قيد التحليل جزءاً أساسياً من النظام الأساسي، مثل نواة نظام التشغيل فقد تكون قيمة النظام عندها مناسبة أكثر).
النظام	S	0,9	يجب أن يتمتع المهاجم بامتيازات إلى النظام الأساسي أو المستضيف المادي المستخدم لتشغيل البرمجية قيد التحليل.
الشبكة	N	0,7	يجب أن يتمتع المهاجم بامتيازات للنفاذ إلى الشبكة.
البنية التحتية للشركة	E	1,0	يجب أن يتمتع المهاجم بامتيازات إلى قطعة بالغة الأهمية من البنية التحتية للشركة، مثل المسيّر، والبدالة، ونظام أسماء الميادين، وجدار الحماية، ومخدّم الهوية، وما إلى ذلك.
افتراضية	D	0,9	متوسط الأوزان الترجيحية للتطبيق، والنظام، والشبكة، والبنية التحتية للشركة.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية ترغب في إنفاذ صارم لفصل الامتيازات حتى بين المستخدمين ذوي الامتيازات بالفعل.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. ويشار إلى أن القيم المحددة كمياً مدعومة من أجل الاكتمال؛ ولكن بما أن الامتيازات والمستخدمين يشكلان كيانات منفصلة فقد تكون هناك حالات محدودة فحسب يكون فيها النموذج المحدد كمياً مفيداً.
ملاحظة – تسهيلاً للتذكر فإن القيم الأساسية لهذا العامل تُختصر بكلمة "SANE" التي تمثل الأحرف الأولى من تسميات هذه القيم باللغة الإنكليزية (System, Application, Network, Enterprise Infrastructure).			

3.4.7 متجه النفاذ (AV)

يحدد متجه النفاذ القناة التي يجب أن يتواصل فيها المهاجم للوصول إلى الشفرة أو الوظيفة المحتوية على موطن الضعف. ويُشار إلى أن هذه القيم مشابهة جداً للقيم المستخدمة في نظام تحديد الدرجات للثغرات الشائعة باستثناء أن نظام تحديد الدرجات لمواطن الضعف الشائعة يميز بين النفاذ المادي والنفاذ المحلي (السطح البيني/الحساب).

ومع أن هناك علاقة وثيقة بين متجه النفاذ وطبقة الامتياز المطلوب فإن الأمرين متمايزان. وعلى سبيل المثال، فقد يكون باستطاعة المهاجم القادر على النفاذ "المادي" إلى المسيّر التأثير على طبقة الشبكة أو الشركة.

الجدول 10 – الأوزان الترجيحية لمتجه النفاذ

القيمة	الرمز	الوزن الترجيحي	الوصف
شبكة الإنترنت	I	1,0	يجب أن يتمتع المهاجم بالقدرة على النفاذ إلى شبكة الإنترنت للوصول إلى موطن الضعف.
شبكة الإنترنت الداخلية	R	0,8	يجب أن يتمتع المهاجم بالقدرة على النفاذ إلى شبكة الإنترنت الداخلية للشركة المحمية من النفاذ المباشر من الإنترنت، وذلك مثلاً باستخدام جدار حماية، على أن النفاذ إلى الشبكة الداخلية بخلاف ذلك متاح لمعظم أفراد الشركة.
شبكة خاصة	V	0,8	يجب أن يتمتع المهاجم بالقدرة عل النفاذ إلى شبكة خاصة يقتصر النفاذ إليها على مجموعة محددة بدقة من الأطراف الموثوقة.
شبكة مجاورة	A	0,7	يجب أن يتمتع المهاجم بالقدرة على النفاذ إلى واجهة مادية إلى الشبكة، مثل ميدان البث أو ميدان التضارب في البرمجية المستهدفة. وتشمل أمثلة الشبكات المحلية شبكة بروتوكول الإنترنت الفرعية المحلية، وBluetooth وIEEE 802.11، ومقطع الإثرنت المحلي.
محلية	L	0,5	يجب أن يكون للمهاجم حساب تفاعلي محلي (سطح بيني) يتفاعل مباشرة مع نظام التشغيل الأساسي.
مادية	P	0,2	يجب أن يتمتع المهاجم بالقدرة على النفاذ المادي إلى النظام الذي يتولى تشغيل البرمجية، أو أن يكون قادراً على التفاعل مع النظام عبر واجهات مثل الناقل التسلسلي الشامل، والقرص المدمج، ولوحة المفاتيح، والفأرة، وما إليها.
افتراضية	D	0,75	متوسط الأوزان الترجيحية للقيم المعنية.
مجهولة	U	0,5	
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. ويشار إلى أن القيم المحددة كمياً مدعومة من أجل الاكتمال؛ ولكن بما أن متجهات النفاذ تشكل كيانات منفصلة فقد تكون هناك حالات محدودة فحسب يكون فيها النموذج المحدد كمياً مفيداً.

4.4.7 شدة الاستيقان (AS)

تغطي شدة الاستيقان شدة إجراء الاستيقان الذي يحمي الشفرة/الوظيفة المحتوية على موطن الضعف.

وحينما يكون هناك أكثر من إجراء واحد للاستيقان قيد الاستخدام، أو إذا ما كان هناك مساران أو أكثر للتشفير، فإن من الواجب تحديد الدرجات على النحو التالي:

- يتم بالنسبة لكل مسار تشفير تحليل إجراء الاستيقان القائم على طول هذا المسار، واختيار القيمة مع أدنى وزن ترجيحي (أي إجراء الاستيقان الأقوى على مسار التشفير). ويُطلق على ذلك اسم قيمة مسار التشفير.
- تُجمع كل قيم مسارات التشفير.
- تُنتقى قيمة مسار التشفير ذات الوزن الترجيحي الأعلى (أي ذات الإجراء الأضعف).

وتُقيِّم هذه الطريقة كل مسار للتشفير من حيث إجراء الاستيقان الأقوى له (حيث إن على المهاجم الالتفاف على هذا الضابط)، ثم تختار مسار التشفير الأضعف (أي الطريق الأسهل بالنسبة للمهاجم).

الجدول 11 – الأوزان الترجيحية لشدة الاستيقان

القيمة	الرمز	الوزن الترجيحي	الوصف
قوية	S	0,7	يتطلب موطن الضعف أقوى طرق متاحة لربط الكيان بهوية من هويات العالم الحقيقي، مثل علامات الاستيقان و/أو الاستيقان متعدد العوامل.
معتدلة	M	0,8	يتطلب موطن الضعف استخدام طرق ذات درجة قوة معتدلة، مثل استخدام الشهادات من سلطات غير الموثوقة، أو الاستيقان المستند إلى المعرفة، أو كلمات السر المستخدمة لمرة واحدة.
ضعيفة	W	0,9	يتطلب موطن الضعف طريقة استيقان بسيطة وضعيفة يمكن الإخلال بها بسهولة باستخدام الانتحال، أو المعجم، أو هجمات التكرار، أو كلمة سر ثابتة.
لا شيء	N	1,0	لا يتطلب موطن الضعف أي استيقان على الإطلاق.
افتراضية	D	0,85	متوسط قيم قوية، ومعتدلة، وضعيفة، ولا شيء.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في بيئة ذات متطلبات ضمان عالية تسعى إلى استئصال كل مواطن الضعف.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

5.4.7 مستوى التفاعل (IN)

يغطي مستوى التفاعل التدابير المطلوبة من الضحية (الضحايا) البشرية للتمكين من تنفيذ هجوم ناجح.

الجدول 12 – الأوزان الترجيحية لمستوى التفاعل

القيمة	الرمز	الوزن الترجيحي	الوصف
مؤتمتة	A	1,0	ليس هناك من داع للتفاعل البشري.
اعتيادية/محدودة	T	0,9	يجب أن يُقنع المهاجم المستخدمَ بالقيام بإجراء شائع أو يعتبر "عادياً" ضمن التشغيل الاعتيادي للمُنتَج. وعلى سبيل المثال، فإن الضغط على حلقة وصل في صفحة شبكية، أو استعراض متن رسالة إلكترونية يعتبر سلوكاً شائعاً.
معتدلة	M	0,8	يجب أن يقنع المهاجم المستخدم بالقيام بإجراء قد يبدو مشبوهاً بالنسبة لمستخدم حذر مستنير. مثلاً: على المستخدم أن يقبل تحذيراً يشير على أن حمولة المهاجم قد تتضمن محتوى خطيراً.
انتهازية	O	0,3	يتعذر على المهاجم أن يتحكم أو يؤثر مباشرةً على الضحية، وبمقدوره فحسب الاستفادة سلبياً من أخطاء أو أفعال الآخرين.
عالية	H	0,1	يتطلب الأمر قدراً كبيراً من الهندسة الاجتماعية، وهو ما يُحتمل أن يتضمن جهل أو إهمال الضحية.
انعدام التفاعل	NI	0,0	ليس هناك من تفاعل ممكن حتى بصورة انتهازية؛ وفي العادة فإن ذلك يحوّل موطن الضعف إلى "خلل" عوضاً عن أن يقود إلى ثغرة. وبما أن الهدف من نظام تحديد الدرجات لمواطن الضعف الشائعة هو الأمن فإن قيمة الوزن الترجيحي هي 0.
افتراضية	D	0,55	متوسط قيم المؤتمتة، والمحدودة، والمعتدلة، والانتهازية، والعالية، وعدم التفاعل.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.

6.4.7 نطاق النشر (SC)

يحدد نطاق النشر ما إذا كان موطن الضعف موجوداً في كل حالات البرمجية القابلة للنشر، أو ما إذا كان مقتصراً على مجموعة فرعية من المنصات و/أو التشكيلات. وعلى سبيل المثال، فإن خطأ الحساب العددي قد ينطبق فحسب على برمجية جارٍ تشغيلها في ظل نظام تشغيل معين ومعمارية 64 بتة، أو قد تؤثر مسألة لعبور المسار فحسب على نظم التشغيل التي تعامل فيها "\" على أنها فاصل دليل.

الجدول 13 – الأوزان الترجيحية لنطاق النشر

القيمة	الرمز (الملاحظة 1)	الوزن الترجيحي	الوصف
الكل	A	1,0	حاضرة في كل المنصات أو التشكيلات.
معتدلة	M	0,9	حاضرة في المنصات أو التشكيلات الشائعة.
نادرة	R	0,5	حاضرة فحسب في المنصات أو التشكيلات النادرة.
يمكن الوصول إليها	P	0,1	يمكن الوصول إليها (الملاحظة 2)، ولكن كل مسارات التشفير آمنة حالياً، و/أو أن موطن الضعف هو في شفرة ميتة.
افتراضية	D	0,7	متوسط الأوزان الترجيحية لقيم RAMP.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. وقد يعرف المستخدم ما هي النسبة المئوية من البرمجية المشحونة (أو المدعومة) المحتوية على الخلل.

الملاحظة 1 – تسهيلاً للتذكر فإن القيم الأساسية لهذا العامل تُختصر بكلمة "RAMP" التي تمثل الأحرف الأولى من تسميات هذه القيم باللغة الإنكليزية (Rare, All, Moderate, Potentially Reachable).

الملاحظة 2 – هناك بعض التداخل بين "يمكن الوصول إليها" و"حقيقية محلياً" في عامل ثقة الكشف.

5.7 فئة المقاييس البيئية

تتألف فئة المقاييس البيئية من العوامل التالية:

- الأثر على الأعمال (BI)
- احتمال الاكتشاف (DI)
- احتمال الاستغلال (EX)
- فعالية الضبط الخارجي (EC)
- الانتشار (P)

1.5.7 الأثر على الأعمال (BI)

يصف الأثر على الأعمال الأثر المحتمل على الأعمال أو المهمة في حال النجاح في استغلال موطن الضعف.

ملاحظة – بما أن شواغل الأعمال تتباين تبايناً شاسعاً بين المنظمات، فإن النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة لا تحاول توفير تقسيم أكثر دقة، وذلك مثلاً من زاوية الأضرار المالية، والمتعلقة بالسمعة، والمادية، والقانونية، أو غير ذلك من أنواع الأضرار. ويمكن تحديد هذا العامل كمياً لمساندة أي نماذج محددة خارجياً.

الجدول 14 – الأوزان الترجيحية للأثر على الأعمال

القيمة	الرمز	الوزن الترجيحي	الوصف
حرجة	C	1,0	يمكن أن تفشل الأعمال/المهمة.
عالية	H	0,9	يمكن أن تتأثر عمليات الأعمال/المهمة بشدة.
متوسطة	M	0,6	يمكن أن تتأثر الأعمال/المهمة، ولكن بدون إلحاق ضرر جسيم بالعمليات العادية.
منخفضة	L	0,3	أثر أدنى على الأعمال/المهمة.
لا شيء	N	0,0	لا أثر على الإطلاق.
افتراضية	D	0,6	متوسط الأوزان الترجيحية لقيم حرجة، وعالية، ومتوسطة، ومنخفضة، ولا شيء.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون هذا العامل منطبقاً في السياقات التي لا يؤبه بها بالأثر على الأعمال، أو إذا كان يجري تقييم الأثر والنظر فيه في عمليات تحليلية خارج نطاق تحديد الدرجات في نظام تحديد الدرجات لمواطن الضعف الشائعة ذاته.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. وقد يكون لبعض المنظمات قياسات معينة لقيمة الأصول فيما يتعلق بالأعمال، مثلاً، وهو ما يمكن أن يُدمج في هذا القياس.

2.5.7 احتمال الاكتشاف (DI)

احتمال الاكتشاف هو احتمال تمكن المهاجم من اكتشاف موطن الضعف.

ملاحظة – جرى النظر في حذف هذا العامل من النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة بالنظر إلى أن من العسير قياسه وأنه يمكن أن يتأثر بعوامل أخرى مثل الامتياز المكتسب، والأثر التقني، والانتشار. على أنه تم الاحتفاظ به مراعاة لأن بعض المطورين سيستخدمون احتمال الاكتشاف للمساعدة في تحديد الأولويات المتعلقة بمدى السرعة التي ينبغي بها إصلاح مسألة ما.

الجدول 15 – الأوزان الترجيحية لاحتمال الاكتشاف

القيمة	الرمز	الوزن الترجيحي	الوصف
عالية	H	1,0	من المحتمل جداً أن يتمكن المهاجم من اكتشاف موطن الضعف بسرعة وبجهد ضئيل باستخدام تقنيات بسيطة، دون النفاذ إلى شفرة المصدر أو الأحداث المصطنعة الأخرى التي تبسط كشف موطن الضعف.
متوسطة	M	0,6	قد يكون بمقدور المهاجم أن يكتشف موطن الضعف، ولكنه يحتاج إلى بعض المهارات للقيام بذلك، كما قد يحتاج إلى النفاذ إلى شفرة المصدر أو إلى معرفة بالهندسة العكسية. وقد يقتضي الأمر بعض الاستثمار الزمني لاكتشاف المسألة.
منخفضة	L	0,2	من المستبعد أن يكتشف المهاجم موطن الضعف دون امتلاكه لمهارات متخصصة رفيعة، والنفاذ إلى شفرة المصدر (أو ما يكافئها)، وقدراً كبيراً من الاستثمار الزمني.
افتراضية	D	0,6	متوسط القيم عالية، ومتوسطة، ومنخفضة.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وقد لا يكون ذلك منطبقاً عندما يفترض واضع الدرجات أن المهاجم سيكتشف كل مواطن الضعف.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

3.5.7 احتمال الاستغلال (EX)

احتمال الاستغلال هو احتمال تمكن مهاجم متمتع بالامتيازات/الاستيقان/النفاذ من أن ينجح في استغلال موطن الضعف عند اكتشافه.

الجدول 16 – الأوزان الترجيحية لاحتمال الاستغلال

القيمة	الرمز	الوزن الترجيحي	الوصف
عالية	H	1,0	من المرجح كثيراً أن يستهدف المهاجم موطن الضعف هذا بنجاح، مع استغلال موثوق قابل للتطوير بسهولة.
متوسطة	M	0,6	من المرجح أن يستهدف المهاجم موطن الضعف هذا بنجاح، غير أن فرص هذا النجاح قد تتباين، أو أنها تتطلب عدة محاولات لتحقيق النجاح.
منخفضة	L	0,2	من المرجح ألا يستهدف المهاجم موطن الضعف هذا، أو أن فرص نجاحه يمكن أن تكون محدودة للغاية.
لا شيء	N	0,0	ليس هناك من فرصة لنجاح المهاجم؛ أي أن المسألة هي "خلل" لأنه ليس هناك من دور للمهاجم أو أنه ليست هناك منفعة للمهاجم.
افتراضية	D	0,6	متوسط قيم عالية، ومتوسطة، ومنخفضة. ويتم تجاهل قيمة "لا شيء" باستثناء أنه سيتم تحديد بضعة كشوف لمواطن الضعف باستخدام هذه القيمة، وسيؤدي إدراجها في الحساب المتوسط إلى خفض الوزن الترجيحي إلى المستوى غير البديهي.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وعلى سبيل المثال، فإن واضع الدرجات قد يرغب في افتراض أن المهاجم يمكن أن يستغل أي موطن ضعف يعثر عليه، أو أنه سيكون على استعداد لاستثمار موارد ضخمة للالتفاف على أي عوائق محتملة لاستغلال النجاح.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

ملاحظة – ويلاحظ أن هذا العامل يتأثر بأثر موطن الضعف لأن المهاجم غالباً ما يستهدف مواطن الضعف التي يكون لها أشد الآثار. وبصورة بديلة فقد يستهدف المهاجم مواطن الضعف التي يسهل تحفيزها. كما أن العامل المذكور يتأثر بالعوامل الأخرى مثل فعالية الضوابط الداخلية والخارجية.

وقد يبدو أن للانتشار تأثيره أيضاً، إلا أن الانتشار يرتبط بصورة أوثق مع احتمال الاكتشاف.

4.5.7 فعالية الضبط الخارجي (EC)

إن فعالية الضبط الخارجي هي قدرة الضوابط أو تدابير التخفيف خارج البرمجية التي قد تزيد من الصعوبات التي يواجهها المهاجم في الوصول إلى موطن الضعف و/أو تحفيزه. وعلى سبيل المثال، فإن تكنولوجيا عشوائية نسق حيز العناوين والتكنولوجيات المماثلة تقلل، ولكنها لا تزيل، فرص نجاح هجوم تدفقات الدارئ. على أن التكنولوجيا المذكورة لا تُستحدث مباشرةً ضمن البرمجية ذاتها.

وحينما تكون هناك ضوابط خارجية متعددة، أو مسارات تشفير متعددة، يمكن أن تصل إلى موطن الضعف ذاته فعندها تطبق التوجيهات التالية:

- يتم بالنسبة لكل مسار تشفير تحليل الضبط الخارجي القائم على طول هذا المسار، واختيار القيمة مع أدنى وزن ترجيحي (أي الضبط الخارجي الأقوى على مسار التشفير). ويُطلق على ذلك اسم قيمة مسار التشفير.
- تُجمع كل قيم مسارات التشفير.
- تُنتقى قيمة مسار التشفير ذات الوزن الترجيحي الأعلى (أي ذات الضبط الأضعف).

وتُقيِّم هذه الطريقة كل مسار للتشفير من حيث الضبط الأقوى له (حيث إن على المهاجم الالتفاف على هذا الضابط)، ثم تختار مسار التشفير الأضعف (أي الطريق الأسهل بالنسبة للمهاجم).

الجدول 17 – الأوزان الترجيحية لفعالية الضبط الخارجي

القيمة	الرمز	الوزن الترجيحي	الوصف
لا شيء	N	1,0	ليس هناك من ضوابط.
محدودة	L	0,9	هناك طرق ساذجة أو قيود عرضية قد تمنع مهاجماً عابراً من استغلال المسألة.
معتدلة	M	0,7	تُستخدم آلية الحماية بشكل عام غير أنها ذات قيود معروفة قد يستطيع المهاجم العارف الالتفاف عليها ببعض الجهد.
غير مباشرة (دفاع في العمق)	I	0,5	لا يوفر الضابط الحماية من استغلال موطن الضعف تحديداً، ولكنه يقلل بصورة غير مباشرة من الأثر عند شن هجوم ناجح. أو أنه يجعل من الصعب إرساء استغلال وظيفي. وعلى سبيل المثال، فإن تكنولوجيا عشوائية نسق حيز العناوين والتكنولوجيات المماثلة تقلل، ولكنها لا تزيل، فرص نجاح هجوم تدفقات الدارئ. وبما أن الاستجابة تتمثل عادة في الخروج من العملية فإن النتيجة تظل رفضاً للخدمة.
أفضل المتوافر	B	0,3	يتَّبع الضابط الممارسات الجارية المثلى، ولو أنه قد يتسم ببعض القيود التي يمكن لمهاجم ماهر ومصمم التغلب عليها، وهو ما قد يتطلب وجود مواطن ضعف أخرى. وعلى سبيل المثال، فإن أمن طبقة النقل (TLS)/طبقة المقابس الآمنة (SSL 3) هو قيد التشغيل على امتداد جانب كبير من شبكة الإنترنت، ولا تتوافر عموماً طرق أقوى بسبب مسائل التوافق.
كاملة	C	0,1	يتسم الضابط بفعالية كاملة إزاء موطن الضعف، أي أنه ليس هناك من خلل أو ثغرة، ولا عواقب وخيمة لاستغلال المسألة. وعلى سبيل المثال، فإن البيئة الافتراضية قد تحصر عمليات النفاذ إلى الملفات بدليل عمل منفرد، وهو ما يوفر الحماية من استغلال عبور المسار. ويُستخدم وزن ترجيحي غير صفري لمراعاة احتمال إزالة الضابط الخارجي عرضاً في المستقبل، وذلك مثلاً في حال تغير بيئة البرمجية.
افتراضية	D	0,6	متوسط قيم كاملة، وأفضل المتوافر، وغير المباشرة، والمعتدلة، والمحدودة، ولا شيء.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية.
محددة كمياً	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة.

5.5.7 الانتشار (P)

يحدد انتشار* كشف ما وتيرة ظهور هذا النمط من موطن الضعف في البرمجية.

ملاحظة – تجدر الإشارة إلى أنه قد يُنظر في حذف هذا العامل من النسخ القادمة. إلا أنه بالنظر إلى ارتباطه المفرط بالطرق العامة لتحديد الدرجات وإطار تحليل أخطار مواطن الضعف الشائعة فإنه لن يُحذف من النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة.

ويُزمع استخدام هذا العامل في الطريقة العامة لتحديد درجات أنواع مواطن الضعف، مثل إعداد قوائم مخصصة بالأخطار الكبرى. وعند تحدد درجات كشف موطن ضعف منفرد في بيئة مسح مؤتمتة فإن هذا العامل سيستخدم على الأرجح قيمة "غير منطبقة".

الجدول 18 – الأوزان الترجيحية للانتشار

القيمة	الرمز	الوزن الترجيحي**	الوصف
واسعة الانتشار	W	1,0	يظهر موطن الضعف في معظم أو في كل البرمجيات في البيئة المصاحبة، وقد يحدث عدة مرات ضمن حزمة البرمجيات ذاته.
عالية	H	0,9	يُلحظ موطن الضعف في كثير من الأحيان، لكنه ليس واسع الانتشار.
شائعة	C	0,8	يظهر موطن الضعف دورياً.
محدودة	L	0,7	يظهر موطن الضعف نادراً، أو قد لا يظهر أبداً.
افتراضية	D	0,85	متوسط قيم محدودة، وشائعة، وعالية، وواسعة الانتشار.
مجهولة	UK	0,5	ليست هناك معلومات كافية لتوفير قيمة لهذا العامل. وقد تدعو الحاجة إلى مزيد من التحليل. وفي المستقبل قد يتم اختيار قيمة مختلفة وهو ما يمكن أن يؤثر على الدرجة.
غير منطبقة	NA	1,0	يجري عمداً تجاهل هذا العامل عند حساب الدرجات لأن لا صلة له بالطريقة التي يرتب فيها واضع الدرجات مواطن الضعف من حيث الأولوية. وعند إجراء تحديد مستهدف للدرجات إزاء كشوف معينة لمواطن الضعف في تطبيق ما، فإن من المتوقع عادة أن يكون الانتشار قيمة لا يؤبه بها، بالنظر إلى أن التطبيق المنفرد والتقنيات التحليلية هما اللذان يحددان وتيرة ظهور موطن الضعف، وستولّد الكثير من الطرق التجميعية لتحديد الدرجات درجات أعلى إذا ما كان هناك عدد أكبر من مواطن الضعف.
محددة كميا	Q		يمكن تحديد هذا العامل باستخدام أوزان ترجيحية مخصصة. وقد تكون بيانات الانتشار الدقيقة متاحة ضمن حالات استخدام محدودة، شريطة أن يتتبع المستخدم بيانات مواطن الضعف بمستوى منخفض من التقسيم. وعلى سبيل المثال، فإن المطوّر قد يتتبع موطن الضعف على امتداد طاقم من المنتجات، أو أن بائع مراجعة التشفير قد يقيس الانتشار من برمجية خاضعة للتحليل على امتداد قاعدة الزبائن. وفي نسخة سابقة من نظام تحديد الدرجات لمواطن الضعف الشائعة حُسب الانتشار استناداً إلى بيانات التصويت الأولية التي جمعت لقائمة Top 25 لعام 2010 التي استخدمت قيماً منفصلة (تتراوح بين 1 و4) تم تعديلها لاحقاً لنطاق يمتد بين 1 و10.
ملاحظة – بما أن بالمستطاع النجاح في مهاجمة البرمجية حتى في حال وجود موطن ضعف منفرد، فإن الأوزان المرجحة المختارة لا توفر تمييزاً مهماً بين بعضها.			

6.7 معادلة درجات نظام تحديد الدرجات لمواطن الضعف الشائعة

يمكن أن تتراوح درجات النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة بين 0 و100. ويمكن حساب هذه الدرجات على النحو التالي:

```
BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore
```

وتتراوح قيم الدرجة الفرعية للكشف القاعدي (BaseFindingSubscore) بين 0 و100. أما الدرجتين الفرعيتين لسطح الهجمات (AttackSurfaceSubscore) والبيئة (EnvironmentSubscore) فتتراوح قيم كلتيهما بين 0 و1.

1.6.7 الدرجة الفرعية للكشف القاعدي

تُحسب الدرجة الفرعية للكشف القاعدي على النحو التالي:

```
Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer) +
5*FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness ] * 4.0

f(TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f(TechnicalImpact) = 1.
```

والقيمة القصوى الممكنة للكشف القاعدي هي 100.

وهناك مكافئ لتعريف f(TechImpact) في نظام تحديد الدرجات للثغرات الشائعة. ويُستخدم هذا التعريف لضمان أنه إذا ما كانت قيمة الأثر التقني 0 فإن العوامل المضافة الأخرى لا تولد عرضاً درجة غير صفرية.

وتُمنح القيمة TechnicalImpact وتوليفةAcquiredPrivilege/AcquiredPrivilegeLayer وزناً ترجيحياً متساوياً، حيث يصل نصيب كل منهما إلى 40% من الدرجة الفرعية للكشف القاعدي. (تولّد كل منهما قيمة فرعية أقصاها 10). وثمة بعض التعديل على ثقة الكشف التي يصل نصيبها إلى 20% من القاعدة (بقيمة قصوى قدرها 5). وبمقدور قيمة InternalControlEffectiveness تعديل الدرجة هبوطاً، وربما حتى 0، رهناً بشدة أية ضوابط داخلية تم تطبيقها على المسألة. وبعد تطبيق قيمة InternalControlEffectiveness فإن النطاق المحتمل للنتائج يتراوح بين 0 و25، بحيث يُستخدم المعامِل 4,0 في تعديل قيمة BaseFindingSubscore إلى نطاق يتراوح بين 0 و100.

2.6.7 الدرجة الفرعية لسطح الهجمات

تُحسب الدرجة الفرعية لسطح الهجمات على النحو التالي:

```
[ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) + 20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0
```

وتشكل توليفة الامتيازات المكتسبة/النفاذ نسبة تصل إلى 60% من الدرجة الفرعية لسطح الهجمات؛ بينما يبلغ نصيب نطاق النشر نسبة 20% أخرى؛ والتفاعل 15%، والاستيقان 5%. ولا تحظى متطلبات الاستيقان بكثير من التركيز وذلك في ظل الافتراض بأن التدقيق القوي للهوية لن يردع المهاجم كثيراً عن محاولة استغلال الثغرة.

ويولِّد ذلك نطاقاً من القيم التي تتراوح بين 0 و100 التي تُقسم بعد ذلك على 100.

3.6.7 الدرجة الفرعية البيئية

تُحسب الدرجة الفرعية البيئية على النحو التالي:

```
[ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit + 3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0
```

```
f(BusinessImpact) = 0 if BusinessImpact == 0; otherwise f(BusinessImpact) = 1
```

ويصل نصيب قيمة BusinessImpact إلى 50% من الدرجة البيئية، ويمكن أن تؤدي إلى تحريك الدرجة النهائية إلى 0. وتكون القيمة ExternalControlEffectiveness غير صفرية على الدوام (لمراعاة خطر إمكانية إزالتها عرضاً إذا ما تغيرت البيئة)، ولكن يمكن أن يكون لها بخلاف ذلك أثر كبير على الدرجة النهائية. ويصل نصيب توليفة LikelihoodOfDiscovery وLikelihoodOfExploit إلى 35% من الدرجة، أما حصة الانتشار فتبلغ 15%.

4.6.7 سمات إضافية للمعادلة

هناك تنوع كبير في أنواع الدرجات التي يمكن تبيانها، إلا أن استخدام مضاعفة العديد من العوامل المختلفة، بالترافق مع أوزان ترجيحية متعددة ذات قيم صغيرة، يعني ميلان نطاق الدرجات المحتملة نحو القيم الأدنى.

وبما أن الوزن الترجيحي للقيمة "غير منطبقة" يبلغ 1، فإن للمعادلة على الدوام درجة قصوى محتملة قدرها 100,0. وفي الحالات شديدة الندرة التي تُعامل فيها بعض العوامل على أنها "غير منطبقة" (مثل الأثر التقني، والأثر على الأعمال، وفعالية الضبط الداخلي)، فإن الدرجة المحتملة الدنيا قد تكون غير صفرية.

وعند استخدام القيم الافتراضية لعدد كبير من العوامل فيما يتعلق بدرجة منفردة، وباستخدام متوسط الأوزان الترجيحية على نحو ما هو محدد في النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة، فإن الدرجات ستميل بشدة نحو الجانب الأدنى. ولا يعكس متوسط الوزن الترجيحي لعامل ما بالضرورة القيمة الأكثر ترجيحاً التي يمكن استخدامها، ولهذا فإن اختيار الأوزان الافتراضية قد يتغير في النسخ المقبلة. وبصورة مثالية فإن المعادلة يجب أن تمتلك خاصية ينتج فيها استخدام العديد من القيم الافتراضية درجة تقترب نسبياً من 50؛ وسيؤدي اختيار قيم غير افتراضية إلى تعديل الدرجة النهائية صعوداً أو هبوطاً، ومن ثم تعزيز الدقة.

وبصورة عامة فإن استخدام قيم "مجهولة" ينتج درجات تميل نحو الجانب الأدنى. وقد يكون ذلك سمة مفيدة، لأن الدرجات ستكون أعلى في حال توافر المزيد من المعلومات الأكثر تحديداً.

7.7 متجهات نظام تحديد الدرجات لمواطن الضعف الشائعة وأمثلة تحديد الدرجات، وقابلية نقل الدرجات

باستخدام الرموز المحددة لكل عامل فإن بالإمكان تخزين درجة نظام تحديد الدرجات لمواطن الضعف الشائعة في صيغة مدمجة، وقابلة للتحليل الآلي، وصالحة للقراءة بشرياً، توفر تفاصيل عن كيفية توليد هذه الدرجة. ويشابه ذلك جداً طريقة بناء متجهات نظام تحديد الدرجات للثغرات الشائعة.

وعلى خلاف نظام تحديد الدرجات للثغرات الشائعة فليس بالمستطاع وصف كل عوامل نظام تحديد الدرجات لمواطن الضعف الشائعة رمزياً بقيم منفصلة. ويمكن تحديد أي عامل كمياً بأوزان ترجيحية متواصلة تطغى على القيم المنفصلة الافتراضية المحددة أصلاً باستخدام القيمة "Q". وعند الحساب باستعمال إطار تحليل أخطار مواطن الضعف الشائعة فإن عامل الأثر هو فعلياً تعبير عن 32 أثراً تقنياً منفصلاً وطبقة منفصلة، والكثير منها لا تنطبق على موطن ضعف معين. ويؤدي التعامل مع كل أثر على أنه عامل منفصل إلى زيادة عدد العوامل التي تتطلب الحساب في درجة نظام تحديد الدرجات لمواطن الضعف الشائعة بمقدار الضعف تقريبا. وفضلاً عن ذلك فإن استخدام إطار تحليل أخطار مواطن الضعف الشائعة لسياق قيمة الأعمال (BVC) في تعديل الدرجات بالنسبة للشواغل المتعلقة تحديداً بالأعمال يعني أيضاً أن درجة نظام تحديد الدرجات لمواطن الضعف الشائعة ومتجهها قد يبدوان كما لو كانا غير متسقين إذا ما "نُقلا" إلى ميادين أو صور مصغرة أخرى.

وبمراعاة هذا الشاغل فإن من المفروض أن يدرج متجه النسخة 1.0 من نظام تحديد الدرجات لمواطن الضعف الشائعة بشكل صريح الأوزان الترجيحية لكل عامل، حتى لو كان ذلك يزيد من حجم تمثيل المتجه.

ونسق العامل المنفرد في متجه نظام تحديد الدرجات لمواطن الضعف الشائعة هو:

اسم العامل (FactorName): القيمة، الوزن

وعلى سبيل المثال، فإن "P:NA,1,0" يحدد قيمة "غير منطبقة" للانتشار بوزن ترجيحي قدره 1,0. ويشير معيِّن النسق "AV:P,0,2" إلى القيمة "المادية" لمتجه النفاذ بوزن ترجيحي قدره 0,2.

وتُفصل العوامل بخط مائل أمامي مثل:

```
AV:I,1.0/RP:G,0.9/AS:N,1.0
```

الذي يدرج القيم والأوزان الترجيحية للقيم "AV" (متجه النفاذ)، و"RP" (مستوى الامتياز المطلوب)، و"AS" (شدة الاستيقان).

وإذا لم يُدرج متجه نظام تحديد الدرجات لمواطن الضعف الشائعة الأوزان الترجيحية الفعلية لقيمة ما، فإنه ينبغي عندها أن يُبلغ التنفيذ عن خطأ أو عدم اتساق، وأن يحاول أن يستخلص صيغة نظام تحديد الدرجات لمواطن الضعف الشائعة بالاستناد إلى عوامل وقيم المتجه، وأن يعيد حساب درجة نظام تحديد الدرجات لمواطن الضعف الشائعة بالاستناد إلى الصيغة المستخلصة، وأن يقارن ذلك بالدرجة الأصلية. وإذا ما كانت الدرجات غير متسقة، فإن على التنفيذ أن يُبلغ عن خطأ أو عدم اتساق محتملين.

1.7.7 مثال: تطبيق بالغ الأهمية للأعمال

لننظر في موطن ضعف مبلغ عنه ويكون التطبيق هو المصدر الرئيسي لدخل شركة ما، ومن ثم فإنه يتسم بقيمة بالغة الأهمية للأعمال. ويتيح التطبيق لمستخدمي الإنترنت العشوائيين التسجيل للحصول على حساب باستخدام عنوان بريدي إلكتروني فحسب. وبمقدور المستخدم عندها استغلال موطن الضعف للحصول على مزايا المدير للتطبيق، غير أن الهجوم لا يمكن أن ينجح إلى أن يطَّلع المدير على تقرير عن أنشطة المستخدمين الأخيرة، وهو حدث شائع. ولا يمكن للمهاجم أن يمتلك السيطرة الكاملة على التطبيق، إلا أن باستطاعته حذف مستخدميه وبياناته. ولنفترض كذلك أنه ليس هناك من ضوابط تمنع حدوث موطن الضعف، إلا أن إصلاح المسألة بسيط، ويقتصر على بضعة سطور من الشفرة.

ويمكن استخلاص الوضع بالمتجه التالي لنظام تحديد الدرجات لمواطن الضعف الشائعة:

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

وقد انقسم المتجه إلى خطوط متعددة تسهيلاً للقراءة. ويمثل كل خط فئة من فئات المقاييس.

وتُعرض العوامل والقيم في الجدول 19 أدناه.

الجدول 19 – العوامل والقيم لمثال تطبيق ذي أهمية بالغة للأعمال

العامل	القيمة
الأثر التقني	عالية
الامتياز المكتسب	مدير
طبقة الامتياز المكتسب	تطبيق
فعالية الضبط الداخلي	لا شيء
ثقة الكشف	حقيقية مثبتة
الامتياز المطلوب	زائر
طبقة الامتياز المطلوب	تطبيق
متجه النفاذ	شبكة الإنترنت
شدة الاستيقان	لا شيء
مستوى التفاعل	اعتيادية/محدودة
نطاق النشر	الجميع
الأثر على الأعمال	بالغ الأهمية
احتمال الاكتشاف	عالية
احتمال الاستغلال	عالية
فعالية الضبط الخارجي	لا شيء
الانتشار	غير منطبقة

ودرجة نظام تحديد الدرجات لمواطن الضعف الشائعة لهذا المتجه هي 92,6، وقد استُخلصت على النحو التالي:

- BaseSubscore (الدرجة الفرعية للكشف القاعدي):

```
o  [ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0
o  f(TI) = 1
o  = [ (10 * 0.9 + 5*(1.0 + 1.0) + 5*1.0) * 1 * 1.0 ] * 4.0
o  = [ (9.0 + 10.0 + 5.0) * 1.0 ] * 4.0
o  = 24.0 * 4.0
o  = 96.0
```

- AttackSurfaceSubscore (الدرجة الفرعية لسطح الهجمات):

```
o  [ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0
o  = [ 20*(0.9 + 1.0 + 1.0) + 20*1.0 + 15*0.9 + 5*1.0 ] / 100.0
o  = [ 58.0 + 20.0 + 13.5 + 5.0 ] / 100.0
o  = 96.5 / 100.0
o  = 0.965
```

- EnvironmentSubscore (الدرجة الفرعية البيئية):
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20.0`
  - `f(BI) = 1`
  - `= [ (10*1.0 + 3*1.0 + 4*1.0 + 3*1.0) * 1 * 1.0 ] / 20.0`
  - `= [ (10.0 + 3.0 + 4.0 + 3.0) * 1.0 ] / 20.0`
  - `= 20.0 / 20.0`
  - `= 1.0`

أما الدرجة النهائية فهي:

`96.0 * 0.965 * 1.0 = 92.64 == 92.6`

2.7.7 مثال: قاعدة بيانات تفاعلية ذات أهمية محدودة بالنسبة للأعمال

لننظر في متجه نظام تحديد الدرجات لمواطن الضعف الشائعة هذا. ولنفترض أن البرمجية هي قاعدة بيانات تفاعلية مستخدمة في تتبع الأحداث الاجتماعية لشركة متوسطة الحجم. وبعض أهم السمات هي أن هناك أثراً تقنياً متوسطاً على مدير للتطبيق من مستخدم عادي للتطبيق، إلا أن هذا التطبيق لا يتسم بأهمية بالغة للأعمال، ومن ثم فإن الأثر الإجمالي على الأعمال منخفض. كما يلاحظ أن قيم معظم عوامل البيئة محددة على أنها "غير منطبقة".

```
(TI:M,0.6/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:RU,0.7/RL:A,1.0/AV:I,1.0/AS:W,0.9/IN:A,1.0/SC:NA,1.0/
BI:L/0.3,DI:NA,1.0/EX:NA,1.0/EC:N,1.0/RE:NA,1.0/P:NA,1.0)
```

وقد انقسم المتجه إلى خطوط متعددة تسهيلاً للقراءة. ويمثل كل خط فئة من فئات المقاييس.

وتُعرض العوامل والقيم في الجدول 20 أدناه.

الجدول 20 – العوامل والقيم لمثال تطبيق ذي أهمية بالغة للأعمال

العامل	القيمة
الأثر التقني	متوسطة
الامتياز المكتسب	مدير
طبقة الامتياز المكتسب	تطبيق
فعالية الضبط الداخلي	لا شيء
ثقة الكشف	حقيقية مثبتة
الامتياز المطلوب	مستخدم عادي
طبقة الامتياز المطلوب	تطبيق
متجه النفاذ	شبكة الإنترنت
شدة الاستيقان	ضعيفة
مستوى التفاعل	مؤتمتة
نطاق النشر	غير منطبقة
الأثر على الأعمال	منخفضة
احتمال الاكتشاف	غير منطبقة
احتمال الاستغلال	غير منطبقة
فعالية الضبط الخارجي	لا شيء
الانتشار	غير منطبقة

ودرجة نظام تحديد الدرجات لمواطن الضعف الشائعة لهذا المتجه هي 51.1، وقد استُخلصت على النحو التالي:

- BaseSubscore (الدرجة الفرعية للكشف القاعدي):
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`
  - `f(TI) = 1`
  - `= [ (10 * 0.6 + 5*(1 + 1) + 5*1) * f(TI) * 1 ] * 4.0`
  - `= 84.0`

- AttackSurfaceSubscore (الدرجة الفرعية لسطح الهجمات):
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0`
  - `= [ 20*(0.7 + 1 + 1) + 20*1.0 + 15*1.0 + 5*0.9 ] / 100.0`
  - `= [ 54.0 + 20.0 + 15.0 + 4.5 ] / 100.0`
  - `= 93.5 / 100.0`
  - `= 0.94 (0.935)`

- EnvironmentSubscore (الدرجة الفرعية البيئية):
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20.0`
  - `f(BI) = 1`
  - `= [ (10*0.3 + 3*1.0 + 4*1.0 + 3*1.0) * f(BI) * 1 ] / 20.0`
  - `= [ (3.0 + 3.0 + 4.0 + 3.0) * 1.0 * 1.0 ] / 20.0`
  - `= [ 13.0 * 1.0 ] / 20.0`
  - `= 0.65`

أما الدرجة النهائية فهي:

```
84.0 * 0.935 * 0.65 = 51.051 == 51.1
```

3.7.7 نُهج أخرى إزاء قابلية نقل درجات نظام تحديد الدرجات لمواطن الضعف الشائعة

عوضاً عن تسجيل كل وزن ترجيحي منفرد ضمن متجه من متجهات نظام تحديد الدرجات لمواطن الضعف الشائعة فإن بالمستطاع اعتماد العديد من الطرق الأخرى.

ومن بين الاحتمالات المطروحة توسيع متجهات نظام تحديد الدرجات لمواطن الضعف الشائعة لتسجيل البيانات الشرحية التي لا تؤثر على الدرجة ولكنها تعرض النسخة أو معلومات مهمة أخرى. ولا حاجة بالضرورة لأن يستخلص جزء البيانات الشرحية الأوزان الترجيحية بحد ذاتها. وعلى سبيل المثال، يمكن تسجيل نسخة نظام تحديد الدرجات لمواطن الضعف الشائعة باستخدام اسم "عامل" مثل "V" إلى جانب قيمة تمثل نسخة ذلك النظام، مثل "V:1.1". وسيؤدي ذلك إلى إضافة 4 بايتات تقريباً إلى كل متجه لنظام تحديد الدرجات لمواطن الضعف الشائعة. على أنه إذا جرى تشفير النسخة ضمن متجه، فلن تدعو الحاجة عندها بعد ذلك إلى تسجيل الأوزان الترجيحية المخصصة (باستثناء القيم المحددة كمياً)، ومن ثم فإن المتجهات الناجمة قد تكون أقصر بكثير.

وهناك نهج مختلف وهو ربط البيانات الشرحية بمجموعة من الدرجات المولَّدة لنظام تحديد الدرجات لمواطن الضعف الشائعة (مثل بطاقة درجات الأثر التقني في حال استخدام إطار تحليل أخطار مواطن الضعف الشائعة)، ولكن سيكون من السهل جداً أن تنفصل هذه البيانات الشرحية عن الدرجات/المتجهات. وسيظل الأمر يقتضي عرض العوامل القابلة للتحديد الكمي ضمن المتجه، بالنظر إلى أنها يمكن أن تتباين بالنسبة لكل كشف من كشوف مواطن الضعف.

وثمة نهج آخر وهو أنه عند نقل درجات نظام تحديد الدرجات لمواطن الضعف الشائعة من طرف إلى آخر فإن بمقدور الطرف المتلقي عندها إعادة حساب الدرجات استناداً إلى المتجهات المعطاة لنظام تحديد الدرجات لمواطن الضعف الشائعة، ثم مقارنة الدرجات المعاد حسابها مع الدرجات الأصلية. وسيشير الاختلاف في الدرجات إلى أن آليات متباينة هي قيد الاستعمال لدى المزوِّد والمتلقي، وربما يكون ذلك نسخة مختلفة من نظام تحديد الدرجات لمواطن الضعف الشائعة.

بيبليوغرافيا

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of Cybersecurity information exchange*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2014), *Common vulnerabilities exposures*.

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-CWRAF] Common Weakness Risk Analysis Framework
<http://cwe.mitre.org/cwraf/>

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020