الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1521

(2011/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل مواطن الضعف/الحالة

نظام تحديد درجات لمواطن الضعف الشائعة

التوصيـــة ITU-T X.1521

الاتحاد الدولي للاتصالات

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
الدليـــل	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
الخصائص البيومترية	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
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

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

التوصيـــة ITU-T X.1521

نظام تحديد درجات لمواطن الضعف الشائعة

ملخص

توفر هذه التوصية المعنية بنظام تحديد درجات لمواطن الضعف الشائعة إطاراً مفتوحاً للتعبير عن خصائص وتأثيرات مواطن ضعف تكنولوجيا المعلومات والاتصالات في برمجيات المصدر المفتوح أو البرمجيات التجارية المستخدمة في شبكات الاتصالات أو أجهزة المستخدم النهائي أو أي من الأنواع الأخرى لتكنولوجيا المعلومات والاتصالات القادرة على تشغيل البرمجيات. والهدف من التوصية هو تمكين مديري تكنولوجيا المعلومات والاتصالات وموردي النشرات المعنية بالثغرات الأمنية وباعة الأمن وباعة التطبيقات والباحثين من التخاطب بلغة مشتركة بشأن نظام تحديد درجات لمواطن الضعف في تكنولوجيا المعلومات والاتصالات.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1521	2011/04/20	17

تمهيـــد

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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظـــة

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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2012

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

المحتـــويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

3 التعاريف 1

1.3 مصطلحات معرفة في أماكن أخرى 1

2.3 مصطلحات معرفة في هذه التوصية 1

4 المختصرات 2

5 اصطلاحات 2

6 استخدام نظام تحديد درجات لمواطن الضعف الشائعة 2

1.6 وصف نظام تحديد درجات لمواطن الضعف الشائعة 3

2.6 كيف يعمل نظام تحديد درجات لمواطن الضعف الشائعة 4

3.6 تقييم علامات نظام تحديد درجات لمواطن الضعف الشائعة 4

4.6 مستخدمو نظام تحديد درجات لمواطن الضعف الشائعة 4

5.6 فئات المقاييس – المقاييس القاعدية 5

6.6 المقاييس الزمنية 8

7.6 المقاييس البيئية 10

8.6 المتجهات القاعدية والزمنية والبيئية 12

9.6 حساب العلامات – المبادئ التوجيهية 12

10.6 المعادلات 13

7 موارد إضافية 15

التذييل I – أمثلة على استخدام نظام تحديد درجات لمواطن الضعف الشائعة (CVSS) 16

1.I CVE-2002-0392 16

1.I CVE-2003-0818 17

3.I CVE-2003-0062 19

التذييل II – موارد إضافية 21

مقدمة

يتعيّن على إدارة تكنولوجيا المعلومات والاتصالات تحديد مواطن الضعف وتقييمها في العديد من منصات العتاد والبرمجيات المختلفة. وبعدئذ ستحتاج الإدارة لتحديد أولويات مواطن الضعف هذه وتدارك ما يشكل الخطر الأكبر منها. وإذ تكثر مواطن الضعف التي يتعين تلافيها، وتُحسب علامة كل منها باستخدام مقاييس مختلفة، يلجأ مدراء تكنولوجيا المعلومات والاتصالات إلى المنهجيات الخاصة بهم للاهتداء إلى سبيل ما لمقارنة مواطن الضعف المتباينة وترجمتها إلى معلومات يتصرفون وفقها.

وبما أن نظام تحديد درجات لمواطن الضعف الشائعة يوحّد النَّهج المتّبع لتشخيص مواطن الضعف، يمكن لمستخدمي هذا النظام أن يحتكموا إلى مقاييس زمنية وبيئية لتطبيق معلومات سياقية تعكس البيئة التي ينفردون بها. ويتيح لهم ذلك اتخاذ قرارات على بيّنة أوضح أثناء سعيهم للتخفيف من المخاطر التي تشكلها مواطن الضعف على أيما بائع في البيئة التي ينفردون بها.

تُعتبر هذه التوصية من الناحية التقنية متكافئة ومتوافقة مع "الإصدار الثاني من نظام تسجيل مواطن الضعف الشائعة (CVSS)" الصادر بتاريخ 20 يونيو 2007، والذي يمكن الاطلاع عليه في الموقع الإلكتروني: http://www.first.org/cvss.

التوصيـــة ITU-T X.1521

نظام تحديد درجات لمواطن الضعف الشائعة

1 مجال التطبيق

تقدم هذه التوصية نهجاً موحداً للتعبير عن خصائص وتأثيرات نقاط ضعف تكنولوجيا المعلومات والاتصالات باستخدام مقاييس زمنية وبيئية تطبق معلومات سياقية تعكس بدقة أكبر مخاطر البيئة التي ينفرد بها كل مستخدم.

تُعتبر هذه التوصية من الناحية التقنية متكافئة ومتوافقة مع "الإصدار الثاني من نظام تحديد درجات لمواطن الضعف الشائعة (CVSS)"، الصادر بتاريخ 20 يونيو 2007، والذي يمكن الاطلاع عليه في الموقع الإلكتروني: http://www.first.org/cvss.

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.

[CVSS Guide] CVSS (2007)، الإصدار 2.0 من دليل نظام تحديد درجات لمواطن الضعف الشائعة <http://www.first.org/cvss/cvss-guide.pdf>

3 التعاريف

1.3 مصطلحات معرفة في أماكن أخرى

1.1.3 موطن الضعف [b-ITU-T X.1500]: أي مواطن ضعف يمكن استغلالها لانتهاك نظام أو المعلومات التي يحتوي عليها.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 النفاذ: قدرة طرف فاعل على رؤية طرف مفعول به وتعديله والتواصل معه. ويتيح النفاذ تدفق المعلومات بين هذين الطرفين.

2.2.3 التيسّر: موثوقية الأفراد المخولين ونفاذهم في الوقت المناسب إلى البيانات والموارد.

3.2.3 السرية: مبدأ أمني يعمل على ضمان عدم الإفصاح عن معلومات لأطراف فاعلة غير مخولة.

4.2.3 الحصانة: مبدأ أمني يضمن عدم تعديل المعلومات والأنظمة بسوء نية أو عرضاً.

5.2.3 الخطر: التأثير النسبي لموطن ضعف مُستغَل على بيئة المستخدم.

6.2.3 التهديد: احتمال أو تواتر وقوع حدث ضار.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

A التأثير من حيث التيسر (*Availability Impact*)

AC تعقيد النفاذ (*Access Complexity*)

AR متطلب التيسر (*Availability Requirement*)

Au الاستيقان (*Authentication*)

AV متجه النفاذ (*Access Vector*)

C التأثير من حيث السرية (*Confidentiality Impact*)

CDP احتمال وقوع أضرار جانبية (*Collateral Damage Potential*)

CR متطلب السرية (*Confidentiality Requirement*)

CVSS نظام تحديد درجات لمواطن الضعف الشائعة (*Common Vulnerability Scoring System*)

DMA النفاذ المباشر إلى الذاكرة (*Direct Memory Access*)

DNS نظام أسماء الميادين (*Domain Name System*)

E التأثير من حيث إمكانية الاستغلال (*Exploitability Impact*)

I التأثير من حيث الحصانة (*Integrity Impact*)

ICT تكنولوجيا المعلومات والاتصالات (*Information and Communication Technologies*)

IM مراسلة فورية (*Instant Messaging*)

IR متطلب الحصانة (*Integrity Requirement*)

JVN مذكرات مواطن الضعف في اليابان (*Japan Vulnerability Notes*)

NVD قاعدة بيانات مواطن الضعف الوطنية (*National Vulnerability Database*)

RC الثقة في التقرير (*Report Confidence*)

RL مستوى التدارك (*Remediation Level*)

RPC نداء الإجراء عن بُعد (*Remote Procedure Call*)

SLA اتفاق مستوى الخدمة (*Service Level Agreement*)

TD توزع الأهداف (*Target Distribution*)

USB الناقل التسلسلي العام (*Universal Serial Bus*)

5 اصطلاحات

لا يوجد.

6 استخدام نظام تحديد درجات لمواطن الضعف الشائعة

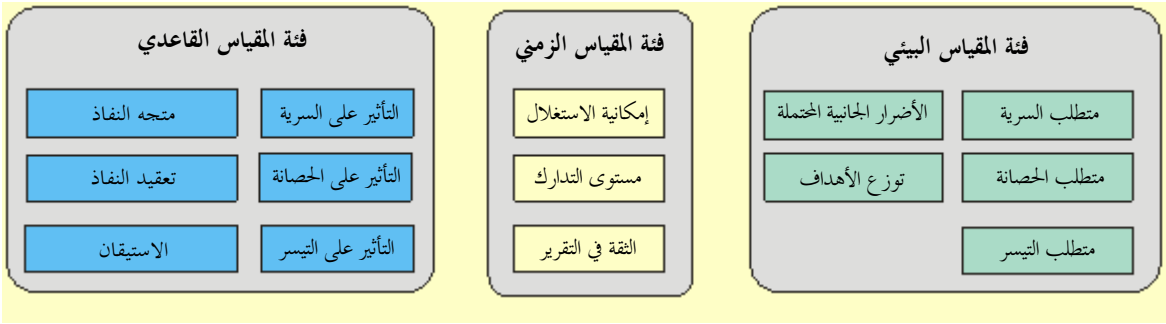
حالياً، تحتاج إدارة تكنولوجيا المعلومات والاتصالات إلى تحديد مواطن الضعف وتقييمها في العديد من منصات العتاد والبرمجيات المختلفة. وتحتاج الإدارة لتحديد أولويات مواطن الضعف هذه وتدارك ما يشكل الخطر الأكبر منها. وإذ تكثر مواطن الضعف التي يتعين تلافيها، وتُحسب علامة كل منها باستخدام مقاييس مختلفة، ويصعب على مديري تكنولوجيا

المعلومات والاتصالات تحويل هذا الركام من بيانات مواطن الضعف إلى معلومات يتصرفون وفقها؟ إن نظام تحديد درجات لمواطن الضعف الشائعة هو إطار مفتوح يتناول هذه القضية. وهو يقدم الفوائد التالية:

- علامات موحدة لمواطن الضعف: عندما تقوم منظمة بتقييس علامات مواطن الضعف لجميع منصات العتاد والبرمجيات لديها، يمكنها الاستفادة من سياسة واحدة لإدارة مواطن الضعف. ويمكن أن تكون هذه السياسة مماثلة لاتفاق مستوى الخدمة التي تنص على مدى سرعة التحقق من مواطن ضعف معينة وتداركها.
- إطار مفتوح: قد يختلط الأمر على المستخدم عند إسناد علامة اعتباطية لموطن ضعف. "فأي خصائص أعطتها هذه العلامة؟ وكيف تختلف عن تلك التي صدرت البارحة؟" باستخدام نظام تحديد درجات لمواطن الضعف الشائعة يمكن لأيّ كان الاطلاع على الخصائص الفردية المستخدمة لاستخلاص العلامة.
- ترتيب أولويات المخاطر: عند حساب العلامة البيئية، يصبح موطن الضعف سياقي. أي أن علامات مواطن الضعف تصبح ممثلةً للمخاطر الفعلية التي تحدق بالمنظمة. فيعرف المستخدمون مدى أهمية موطن ضعف معينة قياساً بمواطن الضعف الأخرى.

1.6 وصف نظام تحديد درجات لمواطن الضعف الشائعة

يتألف النظام المشترك لتحديد درجات لموطن الضعف الشائعة من ثلاث فئات مقاييس: قاعدية وزمنية وبيئية، ويتألف كل منها من مجموعة من المقاييس، على النحو المبين في الشكل 1.



الشكل 1 – فئات مقاييس نظام تحديد درجات لمواطن الضعف الشائعة

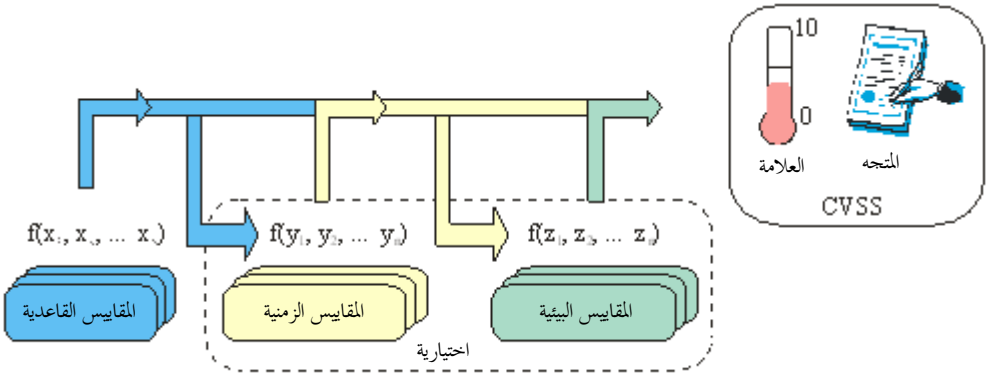
توصف فئات المقاييس على النحو التالي:

- القاعدية: تمثل الخصائص الجوهرية والأساسية لموطن الضعف الثابت على مر الزمن وعبر بيئات المستخدم. وتناقش القياسات القاعدية في الفقرة 5.6.
- الزمنية: تمثل خصائص موطن الضعف الذي يتغير بمرور الوقت ولكن ليس بين بيئات المستخدم. وتناقش المقاييس الزمنية في الفقرة 6.6.
- البيئية: تمثل خصائص موطن الضعف ذو الصلة والذي تنفرد به البيئة الخاصة للمستخدم. وتناقش المقاييس البيئية في الفقرة 7.6.

والغرض من الفئة القاعدية هذه من مقاييس نظام تحديد درجات لمواطن الضعف الشائعة هو تحديد الخصائص الأساسية لموطن الضعف والإعراب عنه. وهذه المقاربة الموضوعية لمواطن الضعف توفر للمستخدمين تمثيلاً واضحاً وبديهياً لموطن الضعف. ثم يمكن للمستخدمين استحضار الفئتين الزمنية والبيئية لتوفير المعلومات السياقية التي تعكس بمزيد من الدقة الخطر الذي تنفرد به بيئتهم. ويتيح لهم ذلك اتخاذ قرارات على بيّنة أوضح أثناء سعيهم للتخفيف من المخاطر التي تشكلها مواطن الضعف.

2.6 كيف يعمل نظام تحديد درجات لمواطن الضعف الشائعة

عند إسناد قيم إلى المقاييس القاعدية، تحسب معادلة القاعدة علامة تتراوح بين صفر وعشرة، ويُنشأ متجه على النحو المبين أدناه في الشكل 2. ويسهل المتجه الطبيعة "المفتوحة" للإطار. وهو سلسلة نصية تحوي القيم المسندة إلى كل مقياس، ويُستخدم للإعراب بدقة عن كيفية استخلاص علامة كل موطن ضعف. ولذلك، ينبغي دائماً عرض المتجه مع علامة موطن الضعف. ويرد شرح إضافي للمتجهات في الفقرة 4.7.



الشكل 2 – مقاييس ومعادلات نظام تحديد درجات لمواطن الضعف الشائعة

يمكن تحسين المقياس القاعدي، حسب الرغبة، بإسناد قيم للمقياسين الزمني والبيئي. ويُستفاد من ذلك لتوفير سياق إضافي لموطن ضعف لإلقاء الضوء، بمزيد من الدقة، على الخطر الذي يشكله موطن الضعف على بيئة المستخدم. ومع ذلك، فهذا ليس مُتطلباً. وتبعاً للغرض المتوخى، قد يكتفى بالعلامة القاعدية والمتجه.

وإذا ما دعت الحاجة لعلامة زمنية، ستجمع المعادلة الزمنية بين المقاييس الزمنية والعلامة القاعدية لإنتاج علامة زمنية تتراوح بين 0 و10. وبالمثل، إذا دعت الحاجة لعلامة بيئية، ستجمع المعادلة البيئية بين المقاييس البيئية والعلامة الزمنية لإنتاج علامة بيئية تتراوح بين 0 و10. ويرد وصف كامل للمعادلات القاعدية والزمنية والبيئية في الفقرة 2.8.

3.6 تقييم علامات نظام تحديد درجات لمواطن الضعف الشائعة

بصفة عامة، يقوم محللو نشرة الثغرات الأمنية أو باعة المنتجات الأمنية أو باعة التطبيقات بتوصيف المقياسين القاعدي والزمني لأنهم أعلم بخصائص مواطن الضعف من المستخدمين. بيد أن المستخدمين يوصّفون المقاييس البيئية لأنهم الأقدر على تقييم الأثر المحتمل لموطن ضعف ضمن بيئاتهم.

4.6 مستخدمو نظام تحديد درجات لمواطن الضعف الشائعة

تستخدم العديد من المنظمات نظام تحديد درجات لمواطن الضعف الشائعة، وتختلف السُّبل التي يجد كل منها قيمة في هذا النظام:

- موردو النشرات المعنية بالثغرات الأمنية: تنشر المنظمات غير الربحية والتجارية على السواء علامات ومتجهات نظام تحديد درجات لمواطن الضعف القاعدية والزمنية في نشراتها المجانية المعنية بالثغرات الأمنية. وتحفل هذه النشرات بالمعلومات، بما في ذلك تاريخ اكتشاف هذه الثغرات والأنظمة المتأثرة بها والوصلات الإلكترونية للباعة المؤدية إلى توصيات الترقيع.
- منافذ بيع تطبيقات البرمجيات: تقدم منافذ بيع تطبيقات البرمجيات لعملائها علامات ومتجهات نظام تحديد درجات لمواطن الضعف القاعدية. ويساعد ذلك عملاءها على التعبير عن شدة الضعف في منتجاتها ويساعدهم على الإدارة الفعالة لمخاطر تكنولوجيا المعلومات والاتصالات التي تخصهم.

- منظمات المستخدمين: تستخدم العديد من منظمات القطاع الخاص نظام تحديد درجات لمواطن الضعف الشائعة داخلياً لاتخاذ قرارات إدارة مواطن الضعف. وهي تستخدم الماسحات أو تكنولوجيات المراقبة لتحديد مواطن الضعف في المضيف والتطبيق. وهي تجمع بين هذه البيانات وبين علامات نظام تحديد درجات علامة مواطن الضعف القاعدية والزمنية والبيئية للحصول على مزيد من معلومات سياقية عن المخاطر ولتدارك مواطن الضعف تلك التي تشكل أكبر خطر على أنظمتهم.
- المسح بحثاً عن موطن الضعف وإدارتها: تمسح منظمات إدارة مواطن الضعف الشبكات بحثاً عن ثغرات أمنية في تكنولوجيا المعلومات والاتصالات. وهي تقدم علامات قاعدية لكل مضيف وفق نظام تحديد درجات علامة مواطن الضعف. وتستعمل منظمات المستخدمين هذا الدّفق الهام من البيانات لإدارة بنيتها التحتية لتكنولوجيا المعلومات والاتصالات على نحو أكثر فعالية بفضل الحد من انقطاعات الخدمة والحماية من التهديدات الخبيثة والعَرَضية ضد تكنولوجيا المعلومات والاتصالات.
- إدارة (المخاطر التي تهدد) الأمن: تستخدم شركات إدارة المخاطر التي تهدد الأمن علامات نظام تحديد درجات لمواطن الضعف الشائعة كمدخل لحساب مستوى المخاطرة أو التهديد في منظمة ما. وتستخدم هذه الشركات التطبيقات المتطورة التي تُدمج في كثير من الأحيان مع طبولوجيا شبكة المنظمة وبيانات مواطن الضعف وقاعدة بيانات المقتنيات لتزويد عملائها بمنظور على بيّنة أوضح من مستوى المخاطر.
- الباحثون: إن الإطار المفتوح لنظام تحديد درجات لمواطن الضعف الشائعة يتيح للأبحاث إجراء تحليل إحصائي لمواطن الضعف وخصائصها.

5.6 فئات المقاييس – المقاييس القاعدية

المقاييس القاعدية تصف فئة المقياس القاعدي الخصائص الثابتة لموطن ضعف على مر الزمن وعبر بيئات المستخدم. ويصف متجه النفاذ وتعقيد النفاذ ومقاييس الاستيقان كيفية النفاذ إلى موطن الضعف، وما إذا كانت شروط إضافية لازمة أم لا لاستغلالها. وتقيس مقاييس التأثير الثلاثة كيف سيؤثر موطن ضعف، إذا استُغلَّ، تأثيراً مباشراً على مقتنيات تكنولوجيا المعلومات والاتصالات، حيث تُعرَّف التأثيرات تعريفاً مستقلاً كدرجة فقدان السرية والحصانة والتيسر. فعلى سبيل المثال، قد يتسبب موطن ضعف بفقدان جزئي للحصانة والتيسر، ولكن دون فقدان السرية.

1.5.6 متجه النفاذ (AV)

يعكس هذا المقياس كيفية استغلال موطن الضعف. وتُدرج القيم الممكنة لهذا المقياس في الجدول 1. وكلما ازدادت إمكانية قيام مهاجم بعيد بالهجوم على المضيف، ارتفعت علامة موطن الضعف.

الجدول 1 – تقييم علامة متجه النفاذ

قيمة المقياس	الشرح
محلية (L)	يتطلب موطن الضعف الذي يمكن استغلاله بنفاذ محلي فقط أن يتمكن المهاجم من النفاذ مادياً إما إلى النظام المستهدف أو إلى حساب محلي (قوقعة). ومن أمثلة مواطن الضعف التي يمكن استغلالها محلياً الهجمات الطرفية عبر سطوح بينية مثل Firewire/USB DMA وأوامر ترفيع للامتياز المحلي (مثل sudo).
شبكة مجاورة (A)	يتطلب موطن الضعف الذي يمكن استغلاله بنفاذ من شبكة مجاورة أن يتمكن المهاجم من النفاذ إلى إما ميدان البث أو ميدان التضارب في البرمجيات المستهدفة. ومن أمثلة الشبكات المحلية، شبكة بروتوكول الإنترنت الفرعية المحلية وBluetooth وIEEE 802.11 ومقطع الإثرنت المحلي.
شبكة (N)	موطن الضعف الذي يمكن استغلاله بنفاذ إلى شبكة يعني أن البرمجيات المستهدفة مسندة إلى كدسة الشبكة ولا يلزم المهاجم نفاذاً إلى الشبكة المحلية أو نفاذاً محلياً. وكثيراً ما يدعى موطن الضعف هذا "قابل للاستغلال عن بُعد". ومن أمثلة هجوم الشبكة، فيض دارئ RPC.

2.5.6 تعقيد النفاذ (AC)

يقيس هذا المقياس تعقيد الهجوم اللازم لاستغلال موطن الضعف حالما ينفذ المهاجم إلى النظام المستهدف. ننظر على سبيل المثال في فيض دارئ في خدمة الإنترنت: فبمجرد تحديد موقع النظام المستهدف، يستطيع المهاجم أن يبادر إلى استغلال الفيض متى شاء.

غير أن استغلال مواطن الضعف الأخرى يمكن أن يتطلب خطوات إضافية. فمثلاً لا يمكن استغلال عميل بريد إلكتروني إلا بعد أن يحمّل المستخدم مرفقاً ملوثاً ويفتحه. وترد القيم الممكنة لهذا المقياس في الجدول 2. فكلما قلّ التعقيد اللازم، ارتفعت علامة موطن الضعف.

الجدول 2 – تقييم علامة تعقيد النفاذ

قيمة المقياس	الشرح
مرتفعة (H)	توجد شروط متخصصة للنفاذ، ومن أمثلتها: • في معظم التشكيلات، يجب أن يتمتع الطرف المهاجم فعلاً بامتيازات مرتفعة أو أن يقلد أنظمة إضافية علاوةً على النظام المهاجم (مثل اختطاف DNS). • يعتمد الهجوم على أساليب الهندسة الاجتماعية التي يكتشفها أُولُو العلم بسهولة. فعلى سبيل المثال، يجب على الضحية القيام بعدة أعمال مشبوهة أو غير نمطية. • يندُرُ جداً أن تصادَف التشكيلة المستهدفة في الممارسة المعملية. • نافذة ضيقة جداً في حال وجود ظرف تسابقي.
متوسطة (M)	شروط النفاذ متخصصة نوعاً ما، ومن أمثلتها ما يلي: • يقتصر الطرف المهاجم على مجموعة من الأنظمة أو المستخدمين عند مستوىً ما من التخويل قد يكون غير موثوق به. • يجب جمع بعض المعلومات قبل التمكُّن من شن هجوم ناجح. • تختلف التشكيلة المتأثرة عن التشكيلة الغيابية، ولا تشكِّل تشكيلاً شائعاً (ومثال ذلك، وجود موطن ضعف عند قيام مخدم بالاستيقان من حساب مستخدم بواسطة خطة معينة، وغياب موطن الضعف هذا في خطة استيقان أخرى). • يتطلب الهجوم قدراً قليلاً من الهندسة الاجتماعية التي قد تخدع المستخدمين الحذرين أحياناً (على سبيل المثال، هجمات التصيّد التي تعدل شريط الحالة في متصفحات الويب لعرض وصلة زائفة، أو وجوب الانضمام إلى قائمة أصدقاء شخص ما قبل إرسال رسائل فورية مستغَلّة).
منخفضة (L)	لا توجد شروط متخصصة للنفاذ أو ظروف مخففة، وفيما يلي أمثلة على ذلك: • يتطلب المنتج المتأثر عادةً النفاذ إلى مجموعة واسعة من الأنظمة والمستخدمين، مما يُحتمل كونه مغفل الهوية وغير موثوق (مثل مخدم الويب المواجه للإنترنت أو مخدم البريد). • التشكيلة المتأثرة تشكيلة غيابية أو منتشرة في كل مكان. • يمكن شن الهجوم يدوياً والأمر لا يتطلب الكثير من المهارة أو جمع معلومات إضافية. • ظرف التسابق يتسم بالكسل (أي يمكن كسب السباق بسهولة من الناحية التقنية).

3.5.6 الاستيقان (Au)

يقيس هذا المقياس عدد المرات التي يجب فيها الاستيقان من مهاجم في الهدف من أجل استغلال موطن الضعف. ولا يقيس هذا المقياس قوة عملية الاستيقان أو تعقيدها، بل مدى إلزام المهاجم بتقديم ثبوتيات قبل وقوع الاستغلال. وتُدرج القيم الممكنة لهذا المقياس في الجدول 3. وكلما قل عدد مرات الاستيقان، ارتفعت علامة موطن الضعف.

الجدول 3 – تقييم علامة الاستيقان

قيمة المقياس	شرح
مرات متعددة (M)	يتطلب استغلال موطن الضعف أن يُستيقن من المهاجم مرتين أو أكثر، حتى لو استُخدمت الثبوتيات نفسها في كل مرة. ومثال ذلك مهاجم يستيقن نظام التشغيل منه، بالإضافة إلى تقديم ثبوتيات المهاجم كي ينفذ إلى تطبيق يحتضنه النظام.
مرة واحدة (S)	يتطلب موطن الضعف أن يكون المهاجم قد سجل دخوله إلى النظام (كما لو بسطر أمر أو عبر دورة سطح مكتب أو عبر سطح بيني في الويب).
ولا مرة (N)	لا يُتطلب الاستيقان لاستغلال موطن الضعف.

ينبغي تطبيق هذا المقياس على أساس الاستيقان الذي يلزم المهاجم قبل أن يشن هجوماً. فعلى سبيل المثال، إذا وُجدت ثغرة أمنية في مخدم بريد تتيح إصدار أمر قبل الاستيقان من مستعمل، ينبغي إسناد علامة "ولا مرة" إلى المقياس لأن المهاجم يمكنه أن يستغل الثغرة قبل استلزام الثبوتيات. أما إذا كان الأمر ذو الثغرة الأمنية متاحاً بعد استيقان ناجح فقط، فينبغي إسناد علامة "مرة واحدة" أو "مرات متعددة" إلى الثغرة تبعاً لعدد مرات الاستيقان الواجب حدوثها قبل إصدار الأمر.

4.5.6 التأثير على السرية (C)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن ضعف على السرية. وتشير السرية إلى تقييد النفاذ إلى المعلومات وعدم الكشف عنها إلا للمستخدمين المخولين، فضلاً عن منع المستخدمين غير المخولين من النفاذ إليها ومنع الإفصاح بها لهم. وتُدرج القيم الممكنة لهذا المقياس في الجدول 4. ويرفع التأثير على السرية من علامة موطن الضعف.

الجدول 4 – تقييم علامة التأثير على السرية

قيمة المقياس	الشرح
معدوم (N)	لا تأثير على سرية النظام.
جزئي (P)	هناك إفشاء ذو شأن للمعلومات. يمكن النفاذ إلى بعض ملفات النظام، إلا أن المهاجم لا يتحكم في ما يحصل عليه أو أن نطاق الخسارة مقيد. ومثال موطن الضعف هذا هو الإفشاء عن جداول معينة فقط في قاعدة بيانات.
كامل (C)	هناك إفصاح عن كامل المعلومات مما يؤدي إلى كشف النقاب عن جميع ملفات النظام. ويتمكن المهاجم من جميع بيانات النظام (الذاكرة والملفات، إلخ).

5.5.6 التأثير على الحصانة (I)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن ضعف على الحصانة. وتشير الحصانة إلى جدارة المعلومات بالثقة وصدقها المضمون. وتُدرج القيمتان الممكنتان لهذا المقياس في الجدول 5. ويرفع التأثير على الحصانة من علامة موطن الضعف.

الجدول 5 – تقييم علامة التأثير على الحصانة

قيمة المقياس	الشرح
معدوم (N)	لا تأثير على حصانة النظام.
جزئي (P)	يمكن تعديل بعض ملفات النظام أو المعلومات، ولكن المهاجم لا يتحكم فيما يمكن تعديله، أو أن نطاق ما يمكن للمهاجم أن يؤثر فيه محدود. فمثلاً، يمكن الكتابة فوق ملفات النظام أو التطبيق أو يمكن تعديلها، سوى أن المهاجم لا يملك أن يؤثر في ملفات بعينها أو أن المهاجم لا يمكنه تعديل الملفات إلا في سياق أو نطاق محدود.
كامل (C)	هناك اختراق كاملٍ لحصانة النظام. وهناك فقدان كامل لحماية النظام مما يؤدي إلى اختراق النظام بأكمله. ويستطيع المهاجم أن يعدل أياً من ملفات النظام المستهدف.

6.5.6 التأثير على التيسُّر (A)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن ضعف على التيسر. ويشير التيسر إلى إمكانية الوصول إلى مصادر المعلومات. وتؤثر كل الهجمات التي تستهلك عرض نطاق الشبكة أو دورات المعالج أو مساحة القرص على تيسر النظام. وتُدرج القيم الممكنة لهذا المقياس في الجدول 6. ويرفع التأثير على التيسر من علامة موطن الضعف.

الجدول 6 – تقييم علامة التأثير على التيسر

قيمة المقياس	الشرح
معدوم (N)	لا تأثير على حصانة النظام.
جزئي (P)	هناك انخفاض في الأداء أو انقطاعات في تيسر الموارد. ومثال ذلك هجوم غامر قائم على الشبكة يسمح بعدد محدود من التوصيلات الناجحة بخدمة الإنترنت.
كامل (C)	هناك إغلاق كامل للمورد المتأثر. ويمكن للمهاجم أن يجعل المورد غير متيسر البتة.

6.6 المقاييس الزمنية

يمكن للتهديد الذي يشكله موطن ضعف أن يتغير مع مرور الوقت. ويلتقط نظام تحديد درجات لمواطن الضعف الشائعة ثلاثة عوامل ذات سياق زمني وهي: تأكيد التفاصيل التقنية لموطن الضعف وحالة استدراك موطن الضعف وتوفر شفرة أو تقنيات استغلال موطن الضعف. وبما أن المقاييس الزمنية اختيارية فإن كل منها يحوي قيمة مقياسية لا تؤثر في العلامة. وتُستخدم هذه القيمة عندما يشعر المستخدم بعدم انطباق مقياس معين على واقعه ويود "تجاوزه".

1.6.6 إمكانية الاستغلال (E)

يقيس هذا المقياس الحالة الحالية لتيسر تقنيات أو شفرة استغلال مواطن الضعف. إذ إن توافر شفرة سهلة الاستخدام للعموم لاستغلال مواطن الضعف يزيد عدد المهاجمين المحتملين بتضمين أولئك غير المهرة منهم، مما يزيد من شدة ضعف الثغرة الأمنية.

وفي البداية، قد يكون استغلال مواطن الضعف أمراً نظرياً ليس إلا في العالم الحقيقي. ويمكن أن يلي ذلك نشر شفرة التنفيذ الأولي لمفهوم استغلال موطن الضعف أو الشفرة الوظيفية أو ما يكفي من التفاصيل التقنية اللازمة لاستغلال موطن الضعف. وعلاوةً على ذلك، يمكن أن تتطور شفرة الاستغلال المتاحة من بيان التنفيذ الأولي للمفهوم إلى شفرة استغلال تنجح في استغلال موطن الضعف باستمرار. وفي الحالات الشديدة، يمكن تسليم هذه الشفرة كحمولة دودة أو فيروسة برمجية قائمة على الشبكة. وتُدرج القيم الممكنة لهذا المقياس في الجدول 7. وكلما سهل استغلال موطن ضعف، ارتفعت علامتها.

الجدول 7 – تقييم علامة تأثير إمكانية الاستغلال

قيمة المقياس	الشرح
غير مثبتة (U)	لا تتوفر شفرة استغلال، أو أن الاستغلال نظري تماماً.
التنفيذ الأولي للمفهوم (POC)	توفر شفرة التنفيذ الأولي للمفهوم أو بيان للهجوم بدون قيمة عملية لهما لمعظم الأنظمة. ويتعذر تشغيل الشفرة أو التقنية في معظم الحالات، وقد تتطلبان تعديلاً كبيراً من جانب مهاجم ماهر.
قابلة للتشغيل (F)	توفر شفرة استغلال قابلة للتشغيل. وتعمل الشفرة في معظم الحالات التي يوجد فيها موطن ضعف.
مرتفعة (H)	إما أن يكون موطن الضعف عرضة للاستغلال بشفرة وظيفية متنقلة مستقلة ذاتياً، أو لا لزوم للاستغلال (لتوفر مشغل يدوي) والتفاصيل متاحة على نطاق واسع. وتعمل الشفرة في كل حالة، أو يجري إيصالها بنشاط عبر وكيل متنقل مستقل ذاتياً (مثل دودة أو فيروس).
غير محددة (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

2.6.6 مستوى التدارك (RL)

يُعدّ مستوى تدارك موطن ضعف عاملاً هاماً في تحديد الأولويات. ولا تكون الثغرة الأمنية مرقعةً عادةً عندما نشرها في البداية. ويمكن للحلول الترقيعية السريعة أن تتدارك الثغرة مرحلياً ريثما تصدر رقعة أو ترقية رسمية. وفي كل مرحلة من هذه المراحل المعنية، تعدَّل العلامة الزمنية تخفيضاً على نحو يعكس تناقص درجة التحسّب حتى يتم الاستدراك كلياً. وتُدرج القيم الممكنة لهذا المقياس في الجدول 8. وكلما قلت درجة الرسمية أو الديمومة للإصلاح، ارتفعت علامة موطن الضعف.

الجدول 8 – تقييم علامة مستوى التدارك

قيمة المقياس	الشرح
إصلاح رسمي (OF)	يتوفر حل كامل من الجهة البائعة. فإما أن تكون الجهة البائعة أصدرت رقعة رسمية، أو أن هناك ترقية متوفرة.
إصلاح مؤقت (TF)	يتوفر إصلاح رسمي ولكنه مؤقت. ويشمل ذلك الحالات التي تُصدر فيها الجهة البائعة إصلاحاً مؤقتاً أو أداة أو ترقيعاً سريعاً.
ترقيع سريع (W)	هناك حل غير رسمي صادر عن غير الجهة البائعة. وفي بعض الحالات، سيبتكر مستخدمو التكنولوجيا المتضررة رقعتهم الخاصة أو سيقدمون سبلاً للالتفاف على الثغرة الأمنية أو التخفيف من ضررها.
غير متوفر (U)	لا يتوفر حل أو يستحيل تطبيقه.
غير محدد (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

3.6.6 الثقة في التقرير (RC)

يقيس هذا المقياس درجة الثقة في وجود موطن ضعف ومصداقية التفاصيل التقنية المعروفة. وفي بعض الأحيان، لا يُعلن على الملأ إلا عن وجود مواطن الضعف دون تفاصيل محددة. ويمكن أن ترد لاحقاً قرائن تدل على موطن الضعف وتؤكَّد بعدئذ بإقرار من الجهة المصدرة أو البائعة للتكنولوجيا المتضررة. ويصبح موطن الضعف أكثر إلحاحاً عندما يُعرف وجودها على وجه اليقين. ويشير هذا المقياس أيضاً إلى مستوى المعرفة التقنية المتاحة لمن يفكرون بالهجوم. وتُدرج القيم الممكنة لهذا المقياس في الجدول 9. وكلما تأكد وجود موطن الضعف من جانب الجهة البائعة أو مصادر موثوقة أخرى، ارتفعت العلامة.

الجدول 9 – تقييم علامة الثقة في التقرير

قيمة المقياس	الشرح
غير مؤكدة (UC)	هناك مصدر واحد غير مؤكد أو ربما عدة تقارير متضاربة. وتقل الثقة في صحة هذه التقارير. ومن الأمثلة على ذلك، إشاعة تطلقها أوساط القرصنة الإلكترونية.
غير مدعومة بقرائن (UR)	هناك عدة مصادر غير رسمية، بما في ذلك ربما شركات أمن أو منظمات بحوث مستقلة. وفي هذه المرحلة، قد تكون هناك تفاصيل تقنية متعارضة أو بعض أوجه الغموض الأخرى العالقة.
مؤكدة (C)	أقرت الجهة المصدرة أو البائعة للتكنولوجيا المتضررة بوجود موطن الضعف الذي يمكن أن يؤكَّد أيضاً بتأكد حدث خارجي كنشر شفرة قابلة للتشغيل في استغلال موطن الضعف أو نشر شفرة التنفيذ الأولي لمفهوم الاستغلال، أو استغلال موطن الضعف فعلاً على نطاق واسع.
غير محددة (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

7.6 المقاييس البيئية

يمكن لبيئات مختلفة أن تؤثر تأثيراً كبيراً على موطن الضعف الذي تعاني منه منظمة وأصحاب المصالح فيها. وتصف فئة المقياس البيئي في نظام تحديد درجات لمواطن الضعف الشائعة خصائص موطن الضعف الذي يرتبط مع بيئة مستخدم تكنولوجيا المعلومات والاتصالات. وبما أن المقاييس البيئية اختيارية، فإن كل منها يحوي قيمة مقياسية لا تؤثر في العلامة. وتُستخدم هذه القيمة عندما يشعر المستخدم بعدم انطباق مقياس معين على واقعه ويود "تجاوزه".

1.7.6 الأضرار الجانبية المحتملة (CDP)

يقيس هذا المقياس احتمالات الخسائر في الأرواح أو المقتنيات المادية جراء الضرر اللاحق بها أو سرقة الممتلكات أو المعدات. ويقيس هذا المقياس أيضاً الخسائر الاقتصادية في الإنتاجية أو الإيرادات. وتُدرج القيم الممكنة لهذا المقياس في الجدول 10. وبطبيعة الحال، كلما ازدادت الأضرار المحتملة، ارتفعت علامة موطن الضعف.

الجدول 10 – تقييم علامة الأضرار الجانبية المحتملة

قيمة المقياس	الشرح
معدومة (N)	لا احتمال لوقوع خسائر في الأرواح أو الأصول المادية أو الإنتاجية أو الإيرادات.
منخفضة (L)	يمكن أن يؤدي الاستغلال الناجح لموطن الضعف هذا إلى أضرار طفيفة للأشخاص أو الممتلكات، أو قد يكبد المنظمة خسارة طفيفة في الإيرادات أو الإنتاجية.
منخفضة إلى متوسطة (LM)	يمكن أن يؤدي الاستغلال الناجح لموطن الضعف هذا إلى أضرار معتدلة للأشخاص أو الممتلكات، أو قد يكبد المنظمة خسارة معتدلة في الإيرادات أو الإنتاجية.
متوسطة إلى مرتفعة (MH)	يمكن أن يؤدي الاستغلال الناجح لموطن الضعف هذا إلى أضرار ذات شأن للأشخاص أو الممتلكات، أو قد يكبد المنظمة خسارة ذات شأن في الإيرادات أو الإنتاجية.
مرتفعة (H)	يمكن أن يؤدي الاستغلال الناجح لموطن الضعف هذا إلى أضرار فادحة للأشخاص أو الممتلكات، أو قد يكبد المنظمة خسارة فادحة في الإيرادات أو الإنتاجية.
غير محددة (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

ومن الواضح أنه يتعين على كل منظمة أن تحدد بنفسها المعنى الدقيق لعبارات "طفيفة ومتوسطة وذات شأن وفادحة".

2.7.6 توزُّع الأهداف (TD)

يقيس هذا المقياس نسبة الأنظمة المعرضة للخطر. والقصد منه أن يكون مؤشراً لبيئة معينة من أجل تقريب النسبة المئوية للأنظمة التي يمكن أن تتأثر بموطن الضعف. وتُدرج القيم الممكنة لهذا المقياس في الجدول 11. وكلما ارتفعت نسبة الأنظمة المعرضة للخطر، ارتفعت العلامة.

الجدول 11 – تقييم علامة توزع الأهداف

قيمة المقياس	الشرح
معدومة (N)	لا توجد أنظمة مستهدفة أو أن الأهداف على درجة عالية من التخصص بحيث لا توجد إلا في بيئة مختبرية. وتنعدم فعلياً النسبة المئوية من البيئة المعرضة للخطر.
منخفضة (L)	توجد أهداف ضمن البيئة ولكن على نطاق ضيق. ما بين 1%-25% من مجمل البيئة معرض للخطر.
متوسطة (M)	توجد أهداف ضمن البيئة ولكن على نطاق متوسط. ما بين 26%-75% من مجمل البيئة معرض للخطر.
مرتفعة (H)	توجد أهداف ضمن البيئة على نطاق واسع. ويُعتبر ما بين 76%-100% من مجمل البيئة معرض للخطر.
غير محددة (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

3.7.6 متطلبات الأمن (AR، IR، CR)

تمكّن هذه المقاييس المحلل من أن يكيّف علامة CVSS تبعاً لأهمية مقتنيات تكنولوجيا المعلومات والاتصالات المتضررة في منظمة المستخدم من حيث السرية والحصانة والتيسر. فإذا كان أحد مقتنيات تكنولوجيا المعلومات والاتصالات داعماً لوظيفة تجارية تولي الأهمية القصوى للتيسر، يستطيع المحلل أن يسند قيمة أكبر للتيسر نسبة إلى السرية والحصانة. ولكل من متطلبات الأمن ثلاث قيم محتملة: منخفضة أو متوسطة أو مرتفعة.

ويُحدَد التأثير الكامل على العلامة البيئية بما يقابل من مقاييس التأثير القاعدية (علماً بأن المقاييس القاعدية للسرية والحصانة والتيسر لا تتغير). أي أن هذه المقاييس تعدل العلامة البيئية من خلال إعادة ترجيح مقاييس تأثير السرية والحصانة والتيسر (القاعدي). فعلى سبيل المثال، يزداد رجحان مقياس تأثير السرية (C) إذا كان متطلب السرية (CR) مرتفعاً. وبالمثل، ينخفض رجحان مقياس تأثير السرية إذا كان متطلب السرية منخفضاً. ويكون رجحان مقياس تأثير السرية حيادياً إذا كان متطلب السرية متوسطاً. ويسري هذا المنطق نفسه على متطلبات الحصانة والتيسر.

وجدير بالذكر أن متطلب السرية لن يؤثر على العلامة البيئية إذا ما انعدم تأثير السرية (القاعدي). كما أن زيادة متطلب السرية لن تغير العلامة البيئية عندما تُسند القيمة الكاملة لمقاييس التأثير (القاعدي). لأن العلامة الفرعية للتأثير (جزء من العلامة القاعدية التي تحسب التأثير) بلغت فعلاً قيمة 10 القصوى.

وتُدرج القيم الممكنة لمتطلبات الأمن في الجدول 12. وللإيجاز، يستخدم الجدول نفسه لجميع المقاييس الثلاثة. وكلما ارتفع متطلب الأمن، ارتفعت العلامة (علماً بأن القيمة المتوسطة هي القيمة الغيابية). وستعدّل هذه المقاييس العلامة بما يصل إلى زائد أو ناقص 2,5.

الجدول 12 – تقييم علامة متطلبات الأمن

قيمة المقياس	الشرح
منخفضة (L)	يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً محدوداً فقط على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء).
متوسطة (M)	يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً جدياً على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء).
مرتفعة (H)	يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً كارثياً على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء).
غير محددة (ND)	إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس.

في العديد من المنظمات، تُصنَّف موارد تكنولوجيا المعلومات والاتصالات وفقاً لحراجتها على أساس موقع الشبكة ووظيفة مصلحة الأعمال واحتمالات الخسائر في العائدات أو الأرواح. فعلى سبيل المثال، تُدرج حكومة الولايات المتحدة كلّ مقتنيات تكنولوجيا المعلومات والاتصالات غير المصنفة في فئة مقتنيات تدعى نظاماً. وإلى كل نظام، يجب إسناد ثلاثة تصنيفات "تأثير محتمل" لإظهار الأثر المحتمل على المنظمة إذا اختُرق النظام وفقاً لأهداف الأمن الثلاثة: السرية والحصانة والتيسر. ومن ثم، فإن كل مقتنيات تكنولوجيا المعلومات والاتصالات غير المصنفة لدى حكومة الولايات المتحدة تصنَّف من حيث التأثير المحتمل تصنيفاً منخفضاً أو معتدلاً أو مرتفعاً فيما يتعلق بأهداف الأمن المتمثلة بالسرية والحصانة والتيسر. ويرد وصف نظام التصنيف هذا ضمن معايير معالجة المعلومات الفدرالية (FIPS) 199. ويتبع نظام تحديد درجات لمواطن الضعف الشائعة هذا النموذج العام لمعايير FIPS 199، ولكنه لا يُلزم المنظمات باستخدام أي نظام معين لإسناد تصنيفات التأثير المنخفض والمتوسط والمرتفع.

8.6 المتجهات القاعدية والزمنية والبيئية

يتألف كل مقياس في المتجه من الاسم المختصر للمقياس متبوعاً بنقطتين ":" ثم بالقيمة المختصرة للمقياس. ويسرد المتجه هذه المقاييس في ترتيب محدد سلفاً باستخدام حرف "/" (الخط المائل) لفصل المقاييس. وفي حال عدم استخدام المقياس الزمني أو البيئي، تُسند إليه قيمة "ND" (غير معرَّف). وتظهر المتجهات القاعدية والزمنية والبيئية في الجدول 13 أدناه.

الجدول 13 – المتجهات القاعدية والزمنية والبيئية

قيمة المقياس	الشرح
قاعدي	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
زمني	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
بيئي	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

مثلاً، موطن الضعف ذو قيم المقياس القاعدي التالية: "متجه النفاذ: قيمة منخفضة، تعقيد: قيمة متوسطة، الاستيقان: لا شيء، تأثير السرية: لا شيء، تأثير الحصانة: جزئي، تأثير التيسر: كامل"، سيكون له المتجه القاعدي التالي: "AV:L/AC:M/Au:N/C:N/I:P/A:C".

9.6 حساب العلامات – المبادئ التوجيهية

ترد أدناه المبادئ التوجيهية التي ينبغي أن تساعد المحللين لدى حساب علامات مواطن الضعف.

1.9.6 اعتبارات عامة

الإرشاد 1 لحساب العلامات: لا ينبغي لحساب علامات مواطن الضعف أن يأخذ في الاعتبار أي تفاعل مع مواطن الضعف الأخرى. أي ينبغي حساب علامة كل موطن ضعف بشكل مستقل.

الإرشاد 2 لحساب العلامات: عند حساب علامة موطن ضعف، انظر في التأثير المباشر على المضيف المستهدف فقط. فمثلاً، انظر في موطن الضعف المتمثل في دس المخطوطات المغرضة في مواقع الويب: فقد يكون تأثيره على نظام المستخدم أكبر بكثير من التأثير على المضيف المستهدف. بيد أن ذلك تأثير غير مباشر. وينبغي حساب مواطن الضعف المتعلقة بدس المخطوطات المغرضة بدون تأثير على السرية أو التيسر، وبتأثير جزئي على الحصانة.

الإرشاد 3 لحساب العلامات: يمكن تشغيل العديد من التطبيقات، مثل مخدمات الويب، بامتيازات مختلفة، وينطوي حساب علامات التأثير على افتراضات بشأن ماهية الامتيازات المستخدمة. ولذلك، ينبغي حساب مواطن الضعف وفقاً للامتيازات الأكثر شيوعاً. سوى أن ذلك لا يعكس بالضرورة الممارسات الأمنية الفضلى، وخاصة بالنسبة لتطبيقات العميل التي تُشغّل في كثير من الأحيان بامتيازات على مستوى الجذر. وفي حال عدم التأكد بشأن أي من الامتيازات هي الأكثر شيوعاً، ينبغي لمحللي حساب العلامات أن يفترضوا التشكيلة الغيابية.

الإرشاد 4 لحساب العلامات: عند حساب تأثير موطن ضعف تتعدد أساليب استغلالها (متجهات الهجوم)، ينبغي للمحلل أن يختار أسلوب الاستغلال الذي يسبب أكبر قدر من التأثير بدلاً من الأسلوب الأكثر شيوعاً أو الأسهل من حيث التنفيذ. فعلى سبيل المثال، في حال وجود شفرة قابلة للتشغيل لاستغلال موطن الضعف في منصة وغيابها في منصة أخرى، ينبغي إسناد قيمة "قابلة للتشغيل" إلى إمكانية الاستغلال. وفي حال وجود تنويعتين مختلفتين لمنتج في تطور متواز (مثل PHP 4.x وPHP 5.x)، ويمكن إصلاح إحدى التنويعتين دون الأخرى، ينبغي أن يُضبط مستوى التدارك بقيمة "غير متوفر".

2.9.6 المقاييس القاعدية

1.2.9.6 متجه النفاذ

الإرشاد 5 لحساب العلامات: عندما يمكن استغلال موطن ضعف محلياً ومن الشبكة على السواء، ينبغي اختيار قيمة "الشبكة". وعندما يمكن استغلال موطن ضعف محلياً ومن الشبكات المجاورة على السواء، ولكن ليس من الشبكات البعيدة، ينبغي اختيار قيمة "شبكة مجاورة". وعندما يمكن استغلال موطن ضعف محلياً ومن الشبكات المجاورة والشبكات البعيدة، ينبغي اختيار قيمة "شبكة".

الإرشاد 6 لحساب العلامات: هناك نقاط ضعف محلية في العديد من تطبيقات العملاء مما يمكن استغلاله عن بُعد إما من خلال إجراءات بمعرفة المستخدم أو عبر المعالجة المؤتمتة. فمثلاً، تقوم برمجيات فك الملفات المضغوطة والماسحات المتقصية للفيروسات بمسح رسائل البريد الإلكتروني الواردة تلقائياً. كما تُستغل التطبيقات المساعدة (أطقم أوفيس، مستعرضات الصور، مشغلات الوسائط، إلخ) عند تبادل الملفات الخبيثة عبر البريد الإلكتروني أو تحميلها من مواقع الإنترنت. ولذلك، ينبغي للمحللين، أن يسندوا علامة "شبكة" إلى متجه النفاذ في مواطن الضعف هذه.

2.2.9.6 الاستيقان

الإرشاد 7 لحساب العلامات: في حال وجود موطن ضعف في خطة الاستيقان نفسها (مثل PAM أو Kerberos) أو في خدمة مغفلة (مثل مخدم FTP عمومي)، ينبغي إسناد علامة "ولا مرة" إلى المقياس لأن المهاجم يمكنه استغلال موطن الضعف دون تقديم ثبوتيات صحيحة. ويمكن اعتبار وجود حساب المستخدم الغيابي استيقاناً "لمرة واحدة" أو "عدة مرات" (عند الاقتضاء)، ولكن إمكانية الاستغلال يمكن أن تكون "مرتفعة" إذا نُشرت الثبوتيات.

الإرشاد 8 لحساب العلامات: يجدر الانتباه إلى أن مقياس الاستيقان يختلف عن متجه النفاذ. وهنا، يُنظر في متطلبات الاستيقان بمجرد النفاذ إلى النظام. وعلى وجه التحديد، بالنسبة إلى مواطن الضعف القابلة للاستغلال محلياً، ينبغي ضبط هذا المقياس بقيمة "مرة واحدة" أو "عدة مرات" إذا كان الاستيقان لازماً بما يتجاوز ما يُتطلب لتسجيل الدخول إلى النظام. ومن أمثلة موطن الضعف القابل للاستغلال محلياً والذي يتطلب الاستيقان هي تلك التي تؤثر في إنصات محرك قاعدة بيانات على مقبس ميدان يونكس (Unix) (أو سطح بيني آخر غير شبكي). فإذا تعين الاستيقان من حق المستخدم باستخدام قاعدة البيانات، ينبغي ضبط هذا المقياس بقيمة "مرة واحدة".

3.2.9.6 تأثيرات السرية والحصانة والتيسر

الإرشاد 9 لحساب العلامات: ينبغي إسناد الفقدان الكامل للسرية والحصانة والتيسر إلى مواطن الضعف التي تتيح نفاذاً على مستوى الجذر، فيما ينبغي إسناد الفقدان الجزئي فقط للسرية والحصانة والتيسر إلى مواطن الضعف التي تتيح نفاذاً على مستوى المستخدم. فعلى سبيل المثال، ينبغي إسناد تأثير كامل للسرية والحصانة والتيسر إلى انتهاك حصانة يسمح لمهاجم بتعديل ملف كلمة مرور في نظام تشغيل.

الإرشاد 10 لحساب العلامات: يمكن أيضاً لمواطن الضعف المسببة لفقدان الحصانة جزئياً أو كلياً أن تؤثر على التيسر. فلعل المهاجم القادر على تعديل السجلات، مثلاً، قادر أيضاً على حذفها.

10.6 المعادلات

يرد أدناه وصف لمعادلات وخوارزميات حساب العلامات لفئات المقاييس القاعدية والزمنية والبيئية. ويرد بحث أوفى في أصل هذه المعادلات واختبارها على العنوان الإلكتروني http://www.first.org/cvss. وترد في التذييل ألف ثلاثة أمثلة عن حالات استخدام هذه المعادلات.

1.10.6 المعادلة القاعدية

المعادلة القاعدية هي أساس علامات النظام المشترك لحساب علامة موطن الضعف (CVSS). أما المعادلة القاعدية (الإصدار 2.10 للصيغة) فهي على النحو التالي:

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20*AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise
AccessVector     = case AccessVector of
                       requires local access: 0.395
                       adjacent network accessible: 0.646
                       network accessible: 1.0
AccessComplexity = case AccessComplexity of
                       high: 0.35
                       medium: 0.61
                       low: 0.71
Authentication   = case Authentication of
                       requires multiple instances of authentication: 0.45
                       requires single instance of authentication: 0.56
                       requires no authentication: 0.704
ConfImpact       = case ConfidentialityImpact of
                       none:             0.000
                       partial:          0.275
                       complete:         0.660
IntegImpact      = case IntegrityImpact of
                       none:             0.000
                       partial:          0.275
                       complete:         0.660
AvailImpact      = case AvailabilityImpact of
                       none:             0.000
                       partial:          0.275
                       complete:         0.660
```

2.10.6 المعادلة الزمنية

إذا ما استُعملت المعادلة الزمنية فهي ستجمع بين المقاييس الزمنية والعلامة القاعدية لإنتاج علامة زمنية تتراوح بين 0 و10. وعلاوةً على ذلك فإن العلامة الزمنية لن تعلو على العلامة القاعدية ولن تكون أدنى منها بأكثر من 33%. والمعادلة الزمنية هي على النحو التالي:

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                *RemediationLevel*ReportConfidence)
Exploitability   = case Exploitability of
                       unproven:             0.85
                       proof-of-concept:     0.90
                       functional:           0.95
                       high:                 1.00
                       not defined:          1.00

RemediationLevel = case RemediationLevel of
                       official-fix:         0.87
                       temporary-fix:        0.90
                       workaround:           0.95
                       unavailable:          1.00
                       not defined:          1.00

ReportConfidence = case ReportConfidence of
                       unconfirmed:          0.90
                       uncorroborated:       0.95
                       confirmed:            1.00
                       not defined:          1.00
```

3.10.6 المعادلة البيئية

إذا ما استُعملت المعادلة البيئية فهي ستجمع بين المقاييس البيئية والعلامة الزمنية لإنتاج علامة بيئية تتراوح بين 0 و10. وعلاوةً على ذلك، فإن هذه المعادلة لن تنتج علامة تعلو على العلامة الزمنية. والمعادلة البيئية هي على النحو التالي:

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact
sub-equation replaced with the AdjustedImpact equation

AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
                 *(1-AvailImpact*AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of
                                 none:            0.0
                                 low:             0.1
                                 low-medium:      0.3
                                 medium-high:     0.4
                                 high:            0.5
                                 not defined:     0.0

TargetDistribution        = case TargetDistribution of
                                 none:            0.00
                                 low:             0.25
                                 medium:          0.75
                                 high:            1.00
                                 not defined:     1.00

ConfReq                     = case ConfReq of
                                 low:             0.5
                                 medium:          1.0
                                 high:            1.51
                                 not defined:     1.0

IntegReq                  = case IntegReq of
                                 low:             0.5
                                 medium:          1.0
                                 high:            1.51
                                 not defined:     1.0

AvailReq                  = case AvailReq of
                                 low:             0.5
                                 medium:          1.0
                                 high:            1.51
                                 not defined:     1.0
```

7 موارد إضافية

يحتوي التذييل II على قائمة بموارد إضافية يمكن أن تكون مفيدة لأي شخص يقوم بتنفيذ بنظام تحديد درجات لمواطن الضعف الشائعة. وتتضمن القائمة مؤشرات لنشرات مواطن الضعف وحاسبات متعددة للنظام CVSS. وتكون نشرات مواطن الضعف مفيدة عند البحث عن معلومات مفصلة حول موطن ضعف معين. كما أن حاسبات النظام CVSS مفيدة عند محاولة حساب العلامات القاعدية أو الزمنية أو البيئية الخاصة بك.

التذييل I

أمثلة على استخدام نظام تحديد درجات لمواطن الضعف الشائعة (CVSS)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

ترد أدناه أمثلة على كيفية استخدام CVSS لثلاثة مواطن ضعف مختلفة.

I.1 CVE-2002-0392

لننظر في CVE-2002-0392: موطن الضعف في التشفير المقطّع المتلفة للذاكرة في مخدّم أباتشي (Apache). في يونيو 2002، اكتُشف موطن ضعف في الوسائل التي يستخدمها مخدّم Apache لمعالجة الطلبات المشفرة باستخدام التشفير المقطّع. وذكرت مؤسسة Apache أن النجاح في استغلال موطن الضعف هذا يمكن أن يؤدي إلى الحرمان من الخدمة في بعض الحالات، وإلى تنفيذ شفرة عشوائية مزودة بامتيازات مخدّم الويب في حالات أخرى.

وبما أن موطن الضعف هذا يمكن أن يُستغل عن بُعد، فإن متجه النفاذ هو "الشبكة". وتعقيد النفاذ "منخفض" لانتفاء الحاجة لظروف إضافية كي ينجح هذا الاستغلال. ولا يحتاج المهاجم إلا لصياغة رسالة الاستغلال المناسبة إلى الجهة المنصتة في شبكة Apache. ولا حاجة لاستيقان لتحريك موطن الضعف (أي مستخدم للإنترنت يمكنه التوصيل بمخدم الويب)، إذن قيمة مقياس الاستيقان هي "معدوم".

وبما أن موطن الضعف هذا يمكن أن يُستغل بأساليب متعددة ذات نتائج مختلفة، يجب وضع علامات لكل أسلوب واستخدام الأعلى بينها.

وإذا ما استُغلّ موطن الضعف لتنفيذ شفرة عشوائية مزودة بأذونات مخدّم الويب بما يسمح بتغيير محتوى الويب وربما الاطلاع على معلومات المستخدم المحلي أو معلومات التشكيلة (بما في ذلك إعدادات التوصيل وكلمات المرور إلى قواعد البيانات الخلفية)، يُضبط مقياسا التأثير على السرية والحصانة بقيمة "جزئي". ويُنتج هذان المقياسان معاً علامة قاعدية قدرها 6,4.

وإذا ما استُغلّ موطن الضعف للتسبّب في الحرمان من الخدمة، يُضبط تأثير التيسر بقيمة "كامل". وتنتج هذه المقاييس معاً علامة قاعدية قدرها 7,8. وبما أن هذه هي أعلى علامة قاعدية ممكنة لخيارات الاستغلال، فإنها تُستخدم بوصفها العلامة القاعدية.

ومن ثم، فإن المتجه القاعدي لموطن الضعف هذه هو: AV:N/AC:L/Au:N/C:N/I:N/A:C.

ومن المعروف أن شفرة الاستغلال موجودة، لذلك تُضبط إمكانية الاستغلال بقيمة "قابلة للتشغيل". وقد نشرت مؤسسة Apache رقعاً لهذه الثغرة الأمنية (متوفرة للإصدارين 1.3 و2.0) إذن مستوى التدارك هو "إصلاح رسمي". وبطبيعة الحال، فإن الثقة في التقرير هي "مؤكدة". وتعدل هذه المقاييس العلامة القاعدية لإعطاء علامة زمنية قدرها 6,4.

وعلى افتراض أن التيسر أكثر أهمية من المعتاد للأنظمة المستهدفة، وتبعاً لقيم الأضرار الجانبية المحتملة وتوزع الأهداف، يمكن أن تتراوح العلامة البيئية بين 0,0 ("معدومة"، "معدوم") و9,2 ("مرتفعة"، "مرتفع"). وتُلخص النتائج أدناه.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Network]              (1.00)
Access Complexity           [Low]                  (0.71)
Authentication              [None]                 (0.704)
Confidentiality Impact      [None]                 (0.00)
Integrity Impact            [None]                 (0.00)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
BASE FORMULA                                   BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = ((0.6*6.9) + (0.4*10.0) - 1.5)*1.176 == (7.8)
-------------------------------------------------------
-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Functional]           (0.95)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
TEMPORAL FORMULA                            TEMPORAL SCORE
-------------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00)                  == (6.4)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [High]                 (1.51)
-------------------------------------------------------
ENVIRONMENTAL FORMULA                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                         == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0) - 1.5)*1.176
                                                 == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0)            == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1})
                                            == (0.00 - 9.2)
-------------------------------------------------------
```

2.I CVE-2003-0818

لننظر في CVE-2003-0818: موطن الضعف في معالجة الأعداد الصحيحة في مكتبة ترميز ASN.1 ضمن برامج مايكروسوفت ويندوز. في سبتمبر 2003، اكتُشف موطن ضعف يستهدف مكتبة ترميز ASN.1 في جميع أنظمة تشغيل مايكروسوفت. وسيؤدي النجاح في استغلال موطن الضعف هذا إلى حالة فيض الدارئ التي تسمح لمهاجم بتنفيذ شفرة عشوائية مزودة بامتيازات إدارة (النظام).

وبما أن موطن الضعف هذا يمكن أن يُستغل عن بُعد، فإن متجه النفاذ هو "الشبكة" و"الاستيقان" "معدوم". وتعقيد النفاذ "منخفض" لانتفاء الحاجة لنفاذ إضافي أو لظروف متخصصة كي ينجح هذا الاستغلال. ويُضبط كل من مقاييس التأثير بقيمة "كامل" بسبب إمكانية الاختراق الكامل للنظام. وتنتج هذه المقاييس بمجملها علامة قاعدية قدرها 10,0.

ومن ثم، فإن المتجه القاعدي لموطن الضعف هذا هو: AV:N/AC:L/Au:N/C:C/I:C/A:C.

ومن المعروف أن شفرة الاستغلال موجودة لموطن الضعف هذا، لذلك تُضبط إمكانية الاستغلال بقيمة "قابلة للتشغيل". وقد نشرت شركة مايكروسوفت في فبراير 2004 الرقعة MS04-007 مما يجعل مستوى التدارك "إصلاحاً رسمياً" والثقة في التقرير "مؤكدة". وتعدل هذه المقاييس العلامة القاعدية لإعطاء علامة زمنية قدرها 8,3.

وعلى افتراض أن التيسر أكثر أهمية من المعتاد للأنظمة المستهدفة، وتبعاً لقيم الأضرار الجانبية المحتملة وتوزع الأهداف، يمكن أن تتراوح العلامة البيئية بين 0,0 ("معدومة"، "معدوم") و9,0 ("مرتفعة"، "مرتفع"). وتُلخص النتائج أدناه.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Network]              (1.00)
Access Complexity           [Low]                  (0.71)
Authentication              [None]                 (0.704)
Confidentiality Impact      [Complete]             (0.66)
Integrity Impact            [Complete]             (0.66)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
FORMULA                                        BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore =((0.6*10.0)+(0.4*10.0) - 1.5)*1.176  == (10.0)
-------------------------------------------------------

-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Functional]           (0.95)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
FORMULA                                     TEMPORAL SCORE
-------------------------------------------------------
round(10.0 * 0.95 * 0.87 * 1.00) ==                 (8.3)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [Low]                   (0.5)
-------------------------------------------------------
FORMULA                                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = 10.41*(1-(1-0.66*1)*(1-0.66*1)
         *(1-0.66*0.5))                          == (9.6)
AdjustedBase =((0.6*9.6)+(0.4*10.0) - 1.5)*1.176
                                                 == (9.7)
AdjustedTemporal == (9.7*0.95*0.87*1.0)          == (8.0)
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1})
                 ==                          (0.00 - 9.0)
-------------------------------------------------------
```

CVE-2003-0062 3.I

لننظر في CVE-2003-0062: فيض الدارئ في برمجيات مكافحة الفيروسات NOD32 التي وضعتها شركة Eset. في فبراير 2003، اكتُشفت ثغرة فيض الدارئ في إصداري Linux وUnix السابقة للإصدار 1.013، وهي ثغرة يمكن أن تسمح للمستخدمين المحليين بتنفيذ شفرة عشوائية مزودة بامتيازات مستخدم ينفّذ برمجيات NOD32. ولتحريك فيض الدارئ، يجب أن ينتظر المهاجم مستخدماً آخر (قد يكون على مستوى الجذر) حتى يمسح مسير دليل مفرط الطول (أو أن يستدرجه إلى ذلك).

وبما أن موطن الضعف هذا لا يمكن أن يُستغل إلا عبر مستخدم مسجَّل في النظام محلياً، فإن متجه النفاذ "محلي". وتعقيد النفاذ "عال" لتعذّر استغلال موطن الضعف هذا وفق نزوات المهاجم. فهناك طبقة إضافية من التعقيد لأن المهاجم يجب أن ينتظر مستخدماً آخر لتشغيل برمجيات المسح بحثاً عن الفيروسات. ويُضبط الاستيقان بقيمة "معدوم" لانتفاء الحاجة للاستيقان من المهاجم في أي نظام إضافي. فإذا ما شغّل مستخدم إداري المسح الباحث عن الفيروسات مسبباً فيض الدارئ، أمكن اختراق النظام اختراقاً كاملاً. وتُضبط مقاييس التأثير الثلاثة بقيمة "كامل" لأن الحالة الأكثر ضرراً يجب أن تؤخذ في الاعتبار. وتنتج هذه المقاييس بمجملها علامة قاعدية قدرها 6,2.

ومن ثم فإن المتجه القاعدي لموطن الضعف هذا هو: AV:L/AC:H/Au:N/C:C/I:C/A:C.

وبما أن شفرة استغلال جزئية قد نُشرت، يُضبط مقياس إمكانية الاستغلال بقيمة "التنفيذ الأولي للمفهوم". وقد نشرت شركة Eset برمجيات محدَّثة مما يجعل مستوى التدارك "إصلاحاً رسمياً" والثقة في التقرير "مؤكدة". وتعدل المقاييس الثلاثة العلامة القاعدية لإعطاء علامة زمنية قدرها 4,9.

وعلى افتراض التساوي التقريبي في أهمية السرية والحصانة والتيسر للأنظمة المستهدفة، وتبعاً لقيم الأضرار الجانبية المحتملة وتوزع الأهداف، يمكن أن تتراوح العلامة البيئية بين 0,0 ("معدومة"، "معدوم") و7,5 ("مرتفعة"، "مرتفع"). وتُلخص النتائج أدناه.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Local]                (0.395)
Access Complexity           [High]                 (0.35)
Authentication              [None]                 (0.704)
Confidentiality Impact      [Complete]             (0.66)
Integrity Impact            [Complete]             (0.66)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
FORMULA                                        BASE SCORE
-------------------------------------------------------
Impact = 10.41 *(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.35*0.704*0.395 == 1.9
f(Impact) = 1.176
BaseScore =((0.6*10)+(0.4*1.9) - 1.5)*1.176      == (6.2)
-------------------------------------------------------
-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Proof-Of-Concept]     (0.90)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
FORMULA                                     TEMPORAL SCORE
-------------------------------------------------------
round(6.2 * 0.90 * 0.87 * 1.00) ==                  (4.9)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [Medium]                (1.0)
-------------------------------------------------------
FORMULA                                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedTemporal == 4.9
EnvScore = round((4.9+(10-4.9)*{0-0.5})*{0-1})
                                          == (0.00 - 7.5)
-------------------------------------------------------
```

التذييل II

موارد إضافية

(لا يشكل هذا التذييل جزءاً أساسياً لهذه التوصية)

نورد أدناه قائمة من الموارد التي قد تكون مفيدة لأي شخص ينفذ نظام تحديد درجات لمواطن الضعف الشائعة (CVSS). ويُستفاد من النشرات المعنية بالثغرات الأمنية عند البحث عن معلومات مفصلة بشأن موطن ضعف معين. ويُستفاد من حاسبات CVSS عند السعي لحساب ما يخصكم من علامات قاعدية أو زمنية أو بيئية.

النشرات المعنية بالثغرات الأمنية:

- يحتفظ المعهد الوطني للمعهد الوطني للمعايير والتكنولوجيا (NIST) بقاعدة البيانات الوطنية للثغرات الأمنية (NVD)، وبموقع نشرة الثغرات الأمنية على الويب الذي يحوي علامات CVSS القاعدية. ويوفر المعهد هذه النشرات على شبكة الإنترنت بالإضافة إلى وصلات تغذية XML للاستخدام مجاناً. ويمكن العثور عليها على العنوانين الإلكترونيين http://nvd.nist.gov/nvd.cfm و http://nvd.nist.gov/download.cfm#XML على التوالي.
- وتنشر أنظمة أمن الإنترنت (ISS) لدى شركة IBM نشرات الثغرات الأمنية X-Force للاستخدام المجاني. وهي تشمل علامات CVSS القاعدية والزمنية، ويمكن الاطلاع عليها عبر العنوان الإلكتروني: http://xforce.iss.net/xforce/alerts.
- وتنشر مؤسسة Qualys مراجع عن الثغرات الأمنية تشمل علامات CVSS القاعدية والزمنية على السواء. ويمكن الاطلاع عليها عبر العنوان الإلكتروني: http://www.qualys.com/research/alerts.
- ويمكن الاطلاع على النشرات المعنية بالثغرات الأمنية لدى شركة سيسكو (Cisco) والتي تشمل علامات CVSS القاعدية والزمنية عبر العنوان الإلكتروني: http://tools.cisco.com/MySDN/Intelligence/home.x. (ملاحظة: يتطلب الأمر حساب توصيل مع سيسكو عبر الإنترنت).
- وتنشر مؤسسة أمن الشبكات المتين (Tenable Network Security) برمجيات تكميلية لأداة المسح بحثاً عن مواطن الضعف Nessus. وتتضمن هذه البرمجيات علامات CVSS القاعدية ويمكن الاطلاع عليها عبر العنوان الإلكتروني: http://www.nessus.org/plugins/.
- وتحتفظ مؤسستا JPCERT/CC وIPA بمذكرات مواطن الضعف في اليابان (JVN)، وهو موقع نشرة مواطن الضعف على الويب التي تشمل علامات CVSS القاعدية. وتوفّر مذكرات JVN يوفر هذه النشرات على شبكة الإنترنت بالإضافة إلى وصلات تغذية XML للاستخدام مجاناً. ويمكن العثور عليها على العنوانين الإلكترونيين http://jvndb.jvn.jp/en/ و http://jvndb.jvn.jp/en/apis/، على التوالي.

حاسبات نظام تحديد درجات لمواطن الضعف الشائعة:

- حاسبة NIST CVSSv2:
  http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
- وكالة ترويج تكنولوجيا المعلومات في اليابان: http://jvndb.jvn.jp/en/cvss/index.html.

بيبليوغرافيا

[b-1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, *CVSS: A Common Vulnerability Scoring System*, National Infrastructure Advisory Council (NIAC), 2004.

[b-2] Microsoft Corporation. *Microsoft Security Response Center Security Bulletin Severity Rating System.* November 2002 [cited 16 March 2007]. Available from URL: `http://www.microsoft.com/technet/security/bulletin/rating.mspx`

[b-3] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cited 16 March 2007]. Available from URL: `http://www.kb.cert.org/vuls/html/fieldhelp`

[b-4] SANS Institute. SANS Critical Vulnerability Analysis Archive. Undated (cited 16 March 2007).

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
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	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) 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
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
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 وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012