|  |  |
| --- | --- |
| **电信标准化局** | **logo_C_** |
|  |  |

 2013年9月30日，日内瓦

|  |  |  |
| --- | --- | --- |
| 文号： | **电信标准化局第52号通函**COM 17/MEU | - 致国际电联各成员国主管部门 |
| 电话：传真：电子邮件： | +41 22 730 5866+41 22 730 5853tsbsg17@itu.int | **抄送：**- ITU-T部门成员；- ITU-T部门准成员；- ITU-T学术成员；- 第17研究组正副主席；- 电信发展局主任；- 无线电通信局主任 |

|  |  |
| --- | --- |
| 事由： | **第17研究组按照世界电信标准化全会（2012年，迪拜）第1号决议第9节的规定为批准ITU-T X.1210、X.1243 Cor.1、X.1546、X.1582和X.1600新建议书草案及ITU-T X.1520和X.1526修订建议书草案而召开的会议2014年1月24日，日内瓦** |

尊敬的先生/女士：

1 应第17研究组（安全）主席的请求，我荣幸地告知您，该研究组将于2014年1月15至24日召开会议，并将采用世界电信标准化全会（2012年，迪拜）第1号决议第9节规定的程序来批准上述建议书草案和勘误草案。

2 建议批准的ITU-T建议书草案的标题、摘要及其出处见**附件1**。

3 所有了解自己或他人持有的专利可能整体或部分地涉及建议批准的（一项或多项）建议书草案内容的国际电联成员国、部门成员、部门准成员或学术机构，均需按照ITU-T/ITU-R/ISO（国际标准化组织）/IEC（国际电工委员会）的共同专利政策，向电信标准化局披露这类信息。

 可通过ITU-T网站（[www.itu.int/ITU-T/ipr/](http://www.itu.int/itu-t/ipr/)）在网上获取已公布的专利信息。

4 考虑到第1号决议第9节的规定，请您在**2014年1月3日**协调世界时24时之前告知我，贵主管部门是否同意授权第17研究组在该研究组会议上审议并批准这些建议书草案和勘误。

如有成员国认为不应进入审议批准程序，应阐明其反对原因并提出可能的修改意见，以推动对相关建议书草案和勘误的进一步审议和批准。

5 如果70％以上的成员国在回复中支持在该研究组会议上审议并批准这些建议书草案和勘误，则将于**2014年1月24日**召开一次全体会议，实施该批准程序。

 为此，我邀请贵主管部门派出代表参加会议。请**国际电联成员国的主管部门**提供其代表团团长的姓名。如果贵主管部门希望由一家经认可的运营机构、一个科学或工业组织或处理电信问题的另一实体作为代表参加会议，则应按照国际电联《公约》第19条第239款的规定，将有关情况适时向主任通报。

6 有关第17研究组会议的议程和所有相关信息将在第3/17号集体函中提供。

7 会后电信标准化局主任将以通函的形式通报就这两份建议书做出的决定。此信息还将在《国际电联操作公报》中公布。

顺致敬意!

电信标准化局主任
马尔科姆•琼森

**附件：1件**

（电信标准化局52号通函）
附件1

案文摘要和出处

ITU-T X.1210（X.trm）新建议书草案“互联网协议网络源安全故障解决机制概述”
COM 17 – R 12

摘要

互联网协议网络中的源故障解决安全问题涉及到用来发现入口点、路径、半路径或造成问题网络事件的一个包或多个包来源的方法，通常用来实施缓解措施。

ITU-T X.1210建议书概述了针对安全问题的源安全故障解决机制以及故障解决机制的选择标准和基本安全导则。

ITU-T X.1243建议书“用于打击垃圾信息的互动网关系统”新勘误1草案
COM 17 – R 13

摘要

ITU-T X.1243（2010年）建议书的此勘误1更正了7.2.7款中的两个错误。

ITU-T X.1520（X.cve）新建议书草案“通用漏洞和暴露”
COM 17 – R 14

摘要

ITU-T X.1520建议书涉及一种交换通用信息安全漏洞和暴露（CVE）的结构性方法，该方法旨在提供在通信网络、最终用户设备或任何其它可运行软件的信息通信技术（ICT）中所使用的商业或开源软件中众所周知问题的通用名称。本建议书的目标是借助该通用命名定义CVE的使用，更加容易地在不同的漏洞能力（工具、存储库、服务）之间分享数据。本建议书旨在定义了CVE的使用，为漏洞数据库和其他能力连结在一起并有助于安全工具和服务的比较提供了一种机制。CVE并不包含风险、影响、调整信息或详细技术信息等信息。CVE只包含标准标识符号码以及状态指示符、简要描述以及对相关漏洞报告和公告的参引。CVE标识符的资料库可查阅[cve.mitre.org/cve/cve.html]。

CVE的目的是在所有众所周知的漏洞和暴露方面做到详尽、全面。尽管CVE有意包含成熟可靠的信息，但其主要重点还是确定由安全工具发现的漏洞和暴露以及为公众所知的任何新问题，并随后解决需要验证的任何陈旧安全问题。

ITU-T X.1526（X.oval）建议书修订草案“开放漏洞和评估语言”
COM 17 – R 15

摘要

ITU-T X.1526建议书 – 开放漏洞和评估语言（OVAL），标准化了评估过程中的三个主要步骤：表示用于测试终点的配置信息；分析终点存在的特定机器状态（脆弱性、配置、补丁状态等）；以及报告评估的结果。OVAL的目标是提供一个国际化的，信息安全领域的社区标准来促进开放和公布可行的安全内容，同时规范这些信息内容在整个安全工具和服务范围的传输。OVAL包括用于对系统细节进行编码的语言，以及整个社区持有的各类内容资料库。

ITU-T X.1546（X.maec）新建议书草案“恶意软件属性列表和特性”
COM 17 – R 16

摘要

“恶意软件属性列表和特性”（MAEC）语言包括提供通用词汇库的恶意软件属性和行为的列表。这些列表属于不同的抽象程度：低级可见物、中级行为和高级分类。作为MAEC初始版本的ITU-T X.1546建议书重点在于创建低级别的恶意软件属性列表并协调该领域已开展的几项类似工作。因此，它首先将有能力确定木马、蠕虫、根工具包等最常见恶意软件类型的特征，但最终将可适用于更为深奥的恶意软件类型。

ITU-T X.1582（X.cybex-tp）新建议书草案“支持网络安全信息交换的传输协议”
COM 17 – R 17

摘要

本建议书概述了已经通过并经过改造用于网络安全信息交换（CYBEX）的传输协议。该建议书概述了传输应用、传输协议特性及安全方面的考虑。

ITU-T X.1600（X.ccsec）新建议书草案“云计算的安全框架”
COM 17 – R 19

摘要

ITU-T X.1600建议书描述了云计算的安全框架。该建议书分析了云计算环境中的安全威胁和挑战并描述了可缓解这些威胁并应对安全挑战的各种安全能力。提供了一种判断这些安全能力中的哪些将需要详细说明缓解云计算安全威胁并应对安全挑战的框架方法。附录I提供了特定的安全威胁或挑战如何通过一种或多种对应的安全能力予以应对的对照表。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_