电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0003-V1.0.0:2018

移动智能终端漏洞威胁评价方法

Evaluation Methods for Smart Mobile Terminal Vulnerability

2018- 03- 01 发布　　2018- 03- 01 实施

电信终端产业协会　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、武汉安天信息技术有限责任公司。

本标准主要起草人：姚一楠，翟世俊，陈传文，陈家林，倪昀泽。

引　　言

随着移动智能终端的普及，用户在享受多种多样的便利功能的同时也面临着越来越多的安全风险。终端系统代码量的增加，引入的漏洞数量和攻击面也随之增加。终端漏洞的威胁程度会随着时间的推移，随着攻击利用慢慢变多而产生变化，而漏洞数量也影响着终端本身的安全性。因此为了更好的评价漏洞的严重程度，以及终端产品的安全性，有必要提出量化计算方法，从而规范产品安全性指标。

本标准从漏洞威胁出发，引入漏洞利用，引用数量等概念评价漏洞威胁等级，并进而通过结合终端漏洞数量，定义产品安全指数，从而得到对移动智能终端安全性的整体评价。

移动智能终端漏洞威胁评价方法

1 范围

本标准规定了移动智能终端漏洞威胁指数，漏洞威胁等级，产品安全指数，产品安全等级四部分评价方法。

本标准适用于各种移动智能终端相关漏洞，各种制式的移动智能终端产品。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 移动智能终端 Smart Mobile Terminal

能够接入移动通信网，具有能够提供应用程序开发接口的开放操作系统，并能够安装和运行应用软件的移动终端。

3.2 缩略语

下列缩略语适用于本文件

CVE	Common Vulnerabilities and Exposures	公共漏洞和暴露
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统

4 评价内容和框架

本标准所针对的目标产品为搭载移动智能操作系统的移动智能终端产品，漏洞评价所针对具有CVE编号的漏洞，其中各评价内容关系如图1所示：

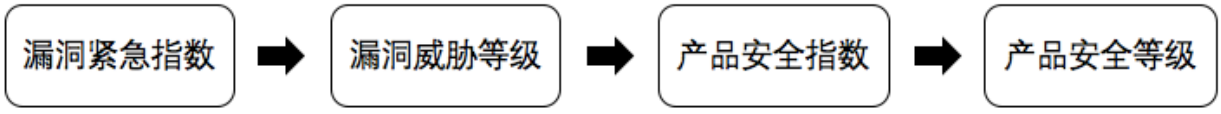


图1 漏洞评价内容及关系

图1中方框部分的内容为移动智能终端漏洞威胁评价内容，整个评价过程为递进关系，后一项评价内容需要依靠前一项作为影响因素之一。漏洞威胁等级要综合漏洞威胁指数进行评价，产品安全指数要根据移动智能终端单个漏洞威胁等级进行评价，产品安全等级要根据产品安全指数进行划分。

5 漏洞紧急指数

5.1 评价要素

漏洞紧急指数定义漏洞对手机造成的危险程度，也反映了漏洞修复的优先级。漏洞威胁的持续性表现在漏洞在从被披露到被利用攻击或被修复的过程中，虽未对手机终端造成实际影响，但存在造成实际影响的机会风险。其机会风险不单纯由漏洞本身的危险性决定，漏洞利用的演进状况也是一个非常重要的因素。所以漏洞紧急指数包含如下要素：

a) 基础分：基础分使用 CVSS 评分体系，采用 v3 版本 Base Scores；

b) 修正分：修正分用于利用其他漏洞评分体系和漏洞利用的演进阶段信息对基础分进行修正。修正分包括静态修正分和动态修正分两部分。

- 静态修正分：静态修正分主要根据其它评价因素对 CVSS V3 进行补充，目前包括漏洞的引用数量和系统厂商的漏洞评级。漏洞的引用数量反映了行业对该漏洞的重视程度，而系统厂商的漏洞评级反映的官方对漏洞的态度。
- 动态修正分：动态修正分参考系统漏洞利用的生命周期的阶段性，选取了几个会显著改变漏洞修正分的重要标志：a. 出现了公开的 PoC，b. 出现了 Exploit，c. 集成到利用工具，d. 出现了利用该漏洞的恶意软件。此外漏洞的 ROOT 能力也对动态修正有一些影响。

5.2 要素赋值

5.2.1 静态修正分

要素	定义	条件	赋值
引用数量	根据漏洞被 cvedetails.com、nvd.nist.gov 公开文档引用的次数进行修正	0	0
		(0,10]	0.1
		(10,20]	0.2
		(20,30]	0.4
		(30,40]	0.6
		(40,50]	0.8
		大于 50	1
厂商评级	根据系统厂商的漏洞评级进行修正	CRITICAL	1
		HIGH	0.5
		MEDIUM	0.2
		LOW	0.1

5.2.2 动态修正分

要素	定义	条件	赋值
漏洞利用	漏洞从披露到产生实际攻击的过程的不同阶段，再赋予不同的权值	未出现任何利用迹象	0
		出现了公开的 PoC	0.3
		出现了 Exploit	0.7
			0.8（是 ROOT 漏洞）
		集成到利用工具	0.95
			1（是 ROOT 漏洞
		出现了相关恶意软件	1

5.3 漏洞紧急指数计算原理

静态修正分＝引用数量 + 厂商评级
动态修正分＝漏洞利用
静态修正结果 =（基础分 + 静态修正分）* 0.75
漏洞紧急指数＝静态修正结果 +（ 12 - 静态修正结果）* 动态修正分

6 漏洞威胁等级

漏洞紧急指数的值在[0,12]之间，根据漏洞紧急指数将漏洞划分为高中低三个等级，如下所述：
——高危漏洞：9-12 分
——中危漏洞：5-8 分
——低危漏洞：0-4 分

7 产品安全指数

7.1 评价要素

产品安全指数反映了一个设备对已知漏洞的修复情况。产品安全指数越高，该设备未修复的漏洞数越少，该设备更安全。产品安全指数是基于漏洞紧急指数、漏洞修复情况、漏洞修复延迟指数等维度对某个设备的安全情况进行评价，提出的产品安全指数的评价方法。需要说明的是，产品安全指数是随着漏洞的披露而变化的。也就是说，产品安全指数只能说明该设备当时的安全情况。

漏洞修复延迟影响指数：漏洞的修复延迟代表移动智能终端在危险状态下运行的时间长度，时间越长意味着移动智能终端的遭受攻击的风险越大。

漏洞影响系数：通过漏洞紧急指数评价结合终端修复的时间延迟，判断终端受单一漏洞的影响大小，漏洞紧急程度约高，修复延迟越大则终端影响越大。

7.2 要素赋值

7.2.1 漏洞修复延迟影响指数

要素	定义	条件	赋值
漏洞修复延迟影响指数	漏洞的修复延迟是当前时间与每个漏洞的操作系统供应商披露时间的差值，以月为单位。以每个修正漏洞的修复延迟单独修正。	低危漏洞	延迟月数/12
		中危漏洞	延迟月数/10
		高危漏洞	延迟月数/8

7.2.2 漏洞影响系数

要素	定义	条件	赋值
漏洞影响系数	单一漏洞对终端产品的影响	低危漏洞	（漏洞紧急指数/12）+ 漏洞修复延迟影响指数
		中危漏洞	
		高危漏洞	

7.3 产品安全指数计算原理

$$产品安全指数 = f(l,m,h) = 100a^{-[0.1\ln(1+\sum_{i=1}^{L} l_i)+0.2\ln(1+\sum_{j=1}^{M} m_j)+1.5\ln(1+\sum_{k=1}^{H} h_k)]}$$

其中：$a = 1.5$，$l_i(i = 1, \cdots L)$表示低危漏洞影响系数，$m_j(j = 1, \cdots M)$表示中危漏洞影响系数，$h_k(k = 1, \cdots H)$表示高危漏洞影响系数，L, M, H分别表示低危、中危和高危漏洞数量。

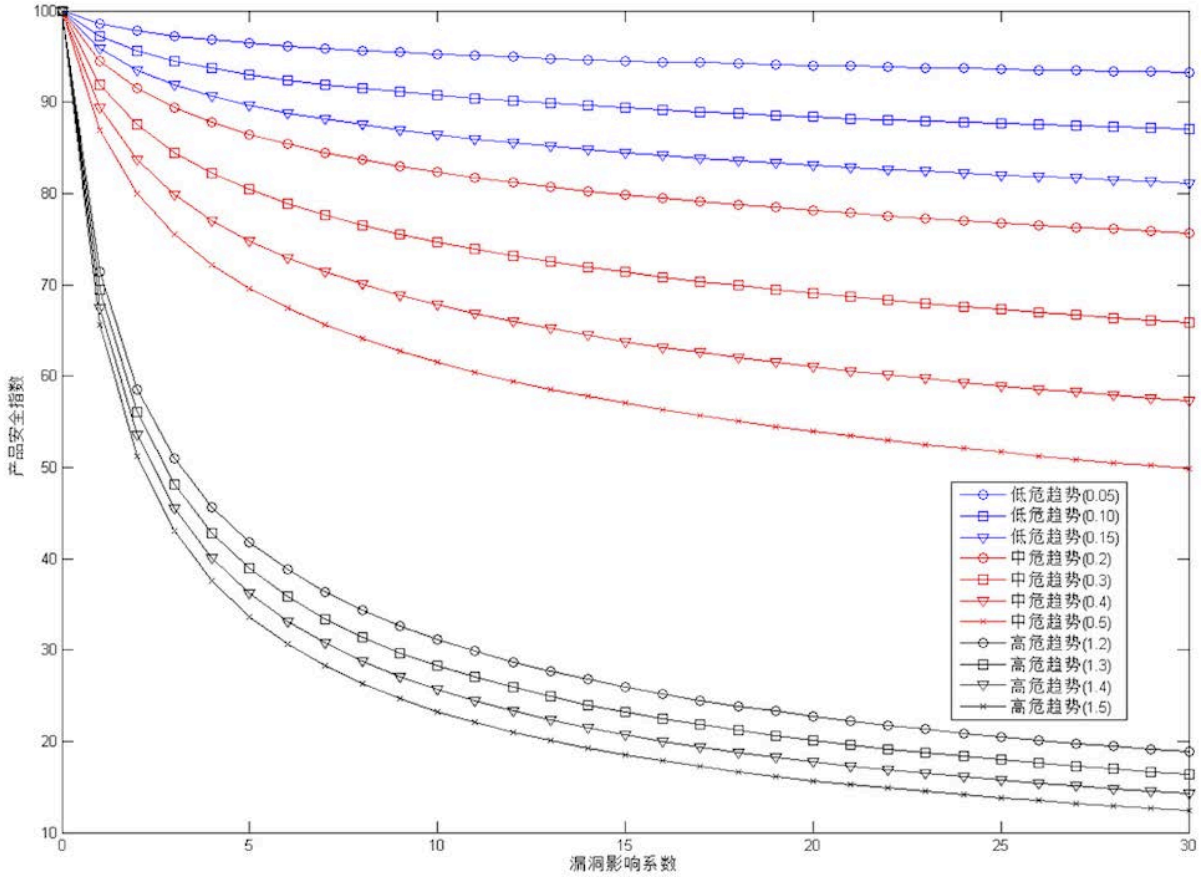
8 产品安全等级

根据产品安全指数将产品划分为高中低三个等级，如下所述：

- 高：产品安全指数大于 80 分。一般威胁等级为高和中的漏洞都已全部修复的移动智能终端的产品安全等级为高；
- 中：产品安全指数大于 60 分，低于 80 分。 一般威胁等级为高的漏洞已全部修复，但威胁指数为中的漏洞尚未全部修复的移动智能终端的产品安全等级为中；
- 低：产品安全指数小于 60。存在威胁等级为高的漏洞尚未修复的移动智能终端的产品安全等级为低。

附　录　A
（资料性附录）
产品安全指数示例

本附录根据标准第7章产品安全指数计算方法，模拟终端漏洞紧急指数和漏洞数量，以示例的形式展现产品安全指数计算过程，以及取值范围。



注：横坐标为产品漏洞数量，纵坐标为产品安全指数，三色曲线依次为终端只含有低危，中危，高危漏洞的趋势。本标准只采用一种取值方法，其余为参考曲线。

图A.1　产品安全指数趋势图

参 考 文 献

[1] GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》；
[2] GB/T 28458-2012 《信息安全技术 安全漏洞标识与描述规范》；