多因素漏洞评价方法研究

杨一未
(中国信息安全测评中心,北京 100085)

摘 要:漏洞引起的网络安全问题日益突出,信息系统运营者和安全技术人员正面临着前所未有的压力,仅凭 CNNVD 等漏洞库给出的漏洞技术等级或评分,无法完全体现漏洞在实际场景中信息资产上的危害程度。该文提出了一种综合计算机系统分级评价、网络防护与联通性、资产使用率、利益相关者风险承受度、漏洞技术评价指标等多种因素的漏洞风险量化评价方法,并给出了详细计算过程。该方法中计算机系统分级评价指标可使用信息安全等级保护指标综合反映系统的重要程度。网络防护与联通性指标进行等级细分后,可定量反映系统受保护程度。资产使用率可通过资产管理系统或在线监测等技术手段获取,反映出系统的影响范围。利益相关者风险承受度指标通过主观打分反映系统风险承受能力。漏洞技术评价指标则通过漏洞客观特性反映危害程度。经模拟数据统计分析显示,该方法能够较全面地分析实际环境中漏洞潜在威胁程度,科学合理地给出不同信息资产上漏洞的消控优先级排序,可供信息系统运营者和安全技术人员用于漏洞危害程度的量化评估。

关键词:漏洞;消控;通用漏洞评分体系;安全;风险
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2022)12-0088-07
doi:10.3969/j.issn.1673-629X.2022.12.014

Research on Multi-factor Vulnerability Scoring System

YANG Yi-wei
(China Information Technology Security Evaluation Center, Beijing 100085, China)

Abstract: Network security problems caused by vulnerabilities are becoming increasingly prominent. Information system operators and security technicians are facing unprecedented pressure. The vulnerability technical grade or score only given by vulnerability databases such as CNNVD cannot fully reflect the damage degree of vulnerabilities on information assets in actual scenarios. Therefore, we propose a quantitative vulnerability risk evaluation method called "multi-factor vulnerability scoring system", which includes five indexes: computer system grading evaluation, network protection and connectivity, asset utilization rate, stakeholder risk tolerance and vulnerability evaluation. In this method, the computer system grading evaluation index can be used to comprehensively reflect the importance of the system by the information security grading protection index. Stakeholder risk tolerance index reflects system risk tolerance through subjective scoring. The vulnerability technology evaluation index reflects the hazard degree through the objective characteristics of vulnerability. The statistical analysis shows that the proposed method can comprehensively analyze the potential threat degree of vulnerabilities in the actual environment, scientifically and reasonably give the priority order of vulnerability control on different information assets, which can be used by information system operators and security technicians to quantitatively evaluate the vulnerability hazard degree. After subdividing the network protection and connectivity indexes, the protection degree of the system can be quantitatively reflected. Asset utilization index can be obtained through asset management system or online monitoring and other technical means to reflect the scope of influence of the system.

Key words: vulnerability; elimination control; common vulnerability scoring system/CVSS; security; risk

0 引 言

2020 年,发生过多起网络信息安全事件,黑客组织“海莲花”对中国 29 个省市的重要卫生医疗机构、应急管理机构等目标对象发起网络间谍活动[1];4 月,美国跨国 IT 服务商 Cognizant 公司遭到 Maze 勒索软件攻击,造成其为客户提供的支持员工远程办公的系统和服务中断;6 月,日本汽车制造商本田的服务器遭到 Ekans 勒索软件攻击,影响了本田的计算机服务器;

收稿日期:2022-01-25 **修回日期**:2022-05-27
基金项目:信息安全国家标准项目经费资助项目(2020BZYJ-WG5-001)
作者简介:杨一未(1978-),男,硕士,高级企业信息管理师,研究方向为信息安全漏洞、漏洞库建设、关键信息基础设施安全、信息安全管理、大数据分析等。

8 月,Maze 勒索软件针对美国和外国政府组织、教育实体、私营公司和卫生机构发起攻击;9 月,阿根廷移民局遭 Ryuk 勒索软件攻击,影响其中央数据中心和分布式服务器的基于 MS Windows 的系统文件[2]。可以看到信息系统运营者和安全技术人员正面临着前所未有的压力,这些安全事件背后或多或少都有信息安全漏洞使用的痕迹。所以信息系统运营者和安全技术人员首先应关注那些漏洞,漏洞危害排序问题变得尤为突出。

目前,使用最为广泛的漏洞风险量化评估方法,是通用漏洞评分体系 CVSS(Common Vulnerability Scoring System)[3],该评分体系是美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)开发,由 FIRST(Forum of Incident Response and Security Teams)维护。该方法由基本组、时间组和环境组三个度量组组成,每一组均含有一套度量指标。基本组的评分范围为 0 至 10,反映漏洞技术指标;时间组反映的是漏洞披露后随着时间的推移、漏洞细节的公布、补丁或修复方案的出现、利用手段的成熟对漏洞危害程度的影响;环境组是供安全人员根据实际场景进行调整的指标,CVSS 只给出了概念性建议。NVD[4] 采用该标准,并在其网站上给出漏洞 CVSS 基础组评分。

中国《GB/T 30279-2020 网络安全漏洞分类分级指南》[5] 的网络安全漏洞分级指标,主要包括被利用性指标、影响程度指标和环境因素指标等三类。网络安全漏洞分级根据漏洞分级的场景不同,分为技术分级和综合分级,每种分级方式均包括超危、高危、中危和低危四个等级。超危漏洞可以非常容易地对目标对象造成特别严重的后果;高危漏洞可以容易地对目标对象造成严重后果;中危漏洞可以对目标对象造成一般后果;低危漏洞可以对目标对象造成轻微后果。其中,技术分级反映特定产品或系统的漏洞危害程度,主要针对漏洞分析人员、产品开发人员等特定产品或系统漏洞的评估工作。综合分级反映在特定时期特定环境下的漏洞危害程度,用于在特定场景下对漏洞危害等级进行划分,主要针对用户对产品或系统在特定网络环境中的漏洞评估工作。漏洞分级过程主要包括指标赋值、指标分级和分级计算三个步骤,其中,指标赋值是将具体漏洞的每个漏洞分级指标进行人工赋值;指标分级是根据指标赋值结果分别对被利用性、影响程度和环境因素等三个指标类进行分级;分级计算是根据指标分级,计算产生技术分级或综合分级的结果。技术分级结果由被利用性和影响程度两个指标类计算产生,综合分级由被利用性、影响程度和环境因素三个指标类计算产生。CNNVD[6] 给出的是依照此标准得出技术分级,该级别与 NVD 给出的 CVSS 基础组评分存在一定的对应关系。

然而,CVSS 和 GB/T 30279-2020 对于信息系统运营者和安全技术人员来讲,在确定环境因素分值上基本采用的都是主观定性打分后进行定量计算的方法,并且这些环境指标变量取决于特定组织机构和特定系统,无法自动生成。该文给出了一种多因素漏洞评价方法(Multi-factor Vulnerability Scoring System,MVSS),并通过实例分析展示了该方法的计算过程。选取 2021 年 CNNVD 发布的若干条公开漏洞,以 CVSS 基础组评分为例,对相同环境指标和不同环境指标下的 MVSS 指数变化曲线、不同漏洞评分数量分布、排序对比情况等进行了统计分析。分析结果表明:同一环境因素下 CVSS 基础组评分曲线与 MVSS 评分曲线波动相同;同一环境因素下 CVSS 基础组评分漏洞数量分布与 MVSS 漏洞评分数量分布相同;在 CVSS 基础组评分分值和环境因素风险度排序相反的情况下,与多因素漏洞评价分值呈反向交叉等现象。但在不同环境因素指标下,呈现出高风险系统中低危漏洞 MVSS 分值高于低风险系统高危漏洞的现象,可见多因素漏洞评价方法可以有效地供信息系统运营者和安全技术人员用于漏洞危害消控排的量化评估。

1　相关研究

桑迪亚国家实验室与美国国土安全部合作发布的《优先考虑网络脆弱性的关键基础设施设备和缓解战略方法》[7-8] 报告,给出一套易受网络攻击的信息资产评价流程,试图寻求最大限度降低这些资产受到攻击带来的损失。Gartner[9] 于 2017 年和 2019 年分别发布了两个版本的《开发和实施漏洞管理指导框架》[10-11],特别是在 2019 年的版本中首次提出了漏洞优先级算法的概念,并指出漏洞优先级计算的重要元素应包括漏洞危害等级、资产暴露情况、威胁上下文、对业务的潜在影响等,但并未给出具体的操作方法。卡耐基梅隆大学的 Jonathan 等人提出了一种可测试的,特定于利益相关者的漏洞分类(Stakeholder-Specific Vulnerability Categorization,SSVC)[12],它对不同的漏洞管理域,采用决策树的形式,分别向补丁开发者和补丁使用者给出漏洞消控紧急程度建议,建议分为推迟(Defer)、排期(Scheduled)、外协(Out-of-Band)、立即(Immediate)四个等级。2021 年 4 月,Jonathan 等人将 SSVC 升级为 2.0 版本[13],2.0 版本中加入了协调利益相关者(Coordinator Stakeholder)角色、调整了术语定义、给出了更为详细的 SSVC 计算方法说明和示例。Dale Peterson 针对工业控制系统(Industrial Control System,ICS)对 SSVC 进行了一定修改,命名为“ICS-

patch”[14]版本定义为 0.5,表明其需要进一步完善的态度,该方法可视为 SSVC 在 ICS 领域的实践。SSVC 和 ICS-patch 方法过于依赖专家判断,定性评价项过多,缺乏实际操作性,也较难实现工程化。黄家辉等人将漏洞风险评估量化指标分为漏洞利用难度和漏洞危害性,同时给出漏洞利用难度打分和漏洞危害性打分,变定性评价为定量指标,利用攻击图来对系统的拓扑结构进行建模分析,以研究每条攻击路径的脆弱性为目标,计算攻击过程中每一步的攻击期望从而得到每条路径的总攻击期望,进而判断漏洞风险[15],但该方法未考虑漏洞固有技术属性和用户群体规模等因素,同时需要确定攻击链后对漏洞攻击图进行分析,分析周期长不利于快速聚焦需关重的漏洞范围。

该文提出的漏洞评价方法,除将漏洞技术评价指标作为漏洞危害消控重要程度考虑因素之外,又加入了计算机系统分级类评价、网络防护与联通性、资产使用率、利益相关者风险承受度四个指标因素,以定量和定性相结合的方法生成信息资产上漏洞危害消控排序,与已有的研究比较更能满足实践要求。

2 评价方法与实例

2.1 MVSS 评价方法

该文提出的多因素漏洞评价方法,通过综合计算机系统分级类评价、网络防护与联通性、资产使用率、利益相关者风险承受度、漏洞技术评价等五类指标,计算得出漏洞消控优先级排序。同时该方法在实际使用过程中漏洞风险评估者还可以根据具体实际情况对评估项进行增减。

表 1 多因素漏洞评价方法(MVSS)指标描述及示例

指标类	指标示例	指标值	指标描述
计算机系统分级类评价	信息安全等级保护五级	5	信息系统受到破坏后,会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查
	信息安全等级保护四级	4	信息系统受到破坏后,会对社会秩序和公共利益造成特别严重损害,或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查
	信息安全等级保护三级	3	信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查
	信息安全等级保护二级	2	信息系统受到破坏后,会对公民、法人和其他组织的合法权益产生严重损害,或者对社会秩序和公共利益造成损害,但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导
	信息安全等级保护一级	1	息系统受到破坏后,会对公民、法人和其他组织的合法权益造成损害,但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护
网络防护与联通性	无保护的互联网访问	5	无任何保护措施的可直接访问互联网的网络
	简单保护的互联网访问	4	仅有防火墙等简单防护手段的可以访问互联网的网络
	复杂保护的互联网访问	3	具备较为完善防护措施的可访问互联网的网络
	逻辑隔离的非互联网访问	2	采用单向或双向网闸逻辑隔离互联网访问的网络
	物理隔离	1	防止来自互联网的攻击采用物理方法将内网与外网隔离的网络。
资产使用率	资产使用率	百分比	某一组织或团体内,使用某一信息系统的人员比例
利益相关者风险承受度	低	5	利益相关者在某一信息系统遭到破会后承受度较低(定性指标)
	中	3	利益相关者在某一信息系统遭到破会后承受度较中等(定性指标)
	高	1	利益相关者在某一信息系统遭到破会后承受度较高(定性指标)
漏洞技术评价	CVSS 基础组评分	CVSS 基础组评分	通过计算漏洞的可利用性和影响度得到,反映漏洞评估的静态分值。

计算机系统分级评价指标是指对信息和信息载体按照重要性等级分级别进行保护而确定的等级,中国普遍使用的是《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》[16]系列标准,美国则可追溯

到由国家计算安全中心(National Computer Security Center,NCSC)制定的可信计算机系统评估准则[17](Trusted Computer System Evaluation Criteria,TCSEC)。该准则于 2014 年 3 月 14 日重新发布为 DoDI 8500.02[18],最终由国际标准化组织 ISO 颁布为《ISO/IEC 15408:2009 Information technology – Security techniques — Evaluation criteria for IT security》系列标准[19-21],该系列标准目前也正在进行改版。网络防护与联通性指标是指信息资产与互联网的连接方式和所采取的防护措施,该指标代表了漏洞通过网络进行攻击的难易程度。资产使用率指标是指某一信息系统使用人员占总人数或使用该系统资产占总资产的比例关系,在某一组织内部,结合资产探测、身份鉴别、上网准入等技术手段该数据可实现自动化统计。利益相关者风险承受度指标是指系统遭到破坏后,信息系统所有者、运营者、用户等的承受度,该指标是 MVSS 统计中唯一定性评价指标。漏洞技术评价指标是指排除环境因素外的漏洞自身危害等级,CVSS 基础组评分就是较好反映漏洞技术评价指标的参考数据值之一,该指标可反映出漏洞的利用难度和攻击者关注程度,同样 GB/T 30279-2020 所给出的漏洞技术分级也可等效使用。MVSS 的详细计算步骤如下:

(1)漏洞评价考虑因素集合为 $X(X \neq \varnothing)$,不同漏洞评价因素初始权重值 $M_i(i \leqslant |X|$,且 $i \in N)$,对漏洞危害等级度 R_i 进行基准化处理:

$$R_i = \frac{M_i}{M_{i+1}} \tag{1}$$

(2)以考虑因素排序最后一项 $K_{|X|}$ 为基准,令其为 1,自下而上依次计算其他评价项目的 K_j 值:

$$K_i = K_{i+1} \times R_i \tag{2}$$

(3)将 K_i 归一化处理,得到权重 W_i:

$$W_i = \frac{K_i}{\sum K_i} \tag{3}$$

(4)资产上发现的漏洞集合 $Y(Y \neq \varnothing)$,$M'_{i,j}(j \leqslant |Y|$,且 $j \in N)$ 是漏洞 V_j 所处第 i 个环境下的具体指标权重,对漏洞危害等级度 $R'_{i,j}$ 进行基准化处理:

$$R'_{i,j} = \frac{M'_{i,j}}{M'_{i,j+1}} \tag{4}$$

(5)令具体环境指标权重排序最后一项 $K'_{i,|Y|}$ 为 1,自下而上依次计算其他评价项目 $K'_{i,j}$ 的值:

$$K'_{i,j} = K'_{i,j+1} \times R'_{i,j+1} \tag{5}$$

(6)将 $K'_{i,j}$ 归一化处理,得到权重 $V_{i,j}$:

$$V_{i,j} = \frac{K'_{i,j}}{\sum_{j=1}^{|Y|} K'_{i,j}} \tag{6}$$

(7)计算漏洞危害消控优先级排序指数 V_j:

$$V_j = \sum_{i=1}^{|X|} W_i \times V_{i,j} \tag{7}$$

(8)对 $V_j(j \leqslant |Y|$,且 $j \in N)$ 从大到小排序,得到漏洞消控优先级排序结果,也可在此基础上划定阈值,对高于该阈值的漏洞重点关注或优先消控。

2.2　评价示例

本节以 Microsoft,CNNVD 编号为 CNNVD-202101-538、CNNVD-202101-792、CNNVD-202101-820、CNNVD-202102-678 的四个漏洞为例,模拟实际环境计算 MVSS 评分,分析 MVSS 在生产环境漏洞风险评估中的有效性。

CNNVD-202101-538(CVE-2020-24003)是 Microsoft Skype 授权问题漏洞,该漏洞允许本地进程获取未经提示的麦克风和摄像头访问,CVSS 得分 3.3,CNNVD 漏洞技术分级为低危;CNNVD-202101-792(CVE-2021-1713)是 Microsoft Excel 缓冲区错误漏洞,CVSS 得分 7.8,CNNVD 漏洞技术分级为高危;CNNVD-202101-820(CVE-2021-1694)是 Microsoft Windows Update Stack 提权漏洞,CVSS 得分 9.8,CNNVD 漏洞技术分级为超危;CNNVD-202102-678(CVE-2021-24085)是 Microsoft Exchange Server 安全漏洞,CVSS 得分 5.5,CNNVD 漏洞技术分级为中危。

现假设上述四个漏洞在不同的四个生产系统中被发现,多因素漏洞评价方法选择的评估指标和漏洞评价因素初始权重如表 2 所示。

表 2　漏洞评价因素初始权重

序号	指标类型	初始权重
1	信息资产等级保护	3
2	网络防护与联通性	3
3	资产使用率	2
4	利益相关者风险承受度	1
5	CVSS 基础组评分	1

根据公式(1)~公式(3),计算 R_i 后,将 K_i 归一化处理,得到权重 W_i,如表 3 所示。

表 3　漏洞评价初始权重归一化

序号	评价项目	R_i	K_i	W_i
1	信息资产等级保护	1	3	0.3
2	网络防护与联通性	1.5	3	0.3
3	资产使用率	2	2	0.2
4	利益相关者风险承受度	1	1	0.1
5	CVSS 基础组评分	–	1	0.1
	合计		10	1

假设不同资产上漏洞的评价项目指标及对应指标值如表 4 所示。

表 4 漏洞评价指标值

Y	信息资产等级保护	网络防护与联通性	资产使用率/%	利益相关者风险承受度	CVSS 基础组评分
CNNVD-202101-538	二级(2)	无保护的互联网访问(5)	60	低(1)	3.3
CNNVD-202101-792	三级(3)	简单保护的互联网访问(4)	40	低(1)	7.8
CNNVD-202101-820	一级(1)	复杂保护的互联网访问(3)	80	中(3)	9.8
CNNVD-202102-678	四级(4)	物理隔离(1)	20	高(5)	5.5

根据公式(4)~公式(6),对漏洞危害等级度 $R_{i,j}^{'}$ 一化处理后,得到权重 $V_{i,j}$ 值,计算结果如表 5 所示。进行基准化处理,依次计算评价项目 $K_{i,j}^{'}$ 值,将 $K_{i,j}^{'}$ 归

表 5 漏洞权重归一化

序号	评价项目	资产漏洞	$R_{i,j}^{'}$	$K_{i,j}^{'}$	$V_{i,j}$
1	信息资产等级保护	CNNVD-202101-538	0.667	0.500	0.2
		CNNVD-202101-792	3.000	0.750	0.3
		CNNVD-202101-820	0.250	0.250	0.1
		CNNVD-202102-678		1	0.4
	合计			2.5	1
2	网络防护与联通性	CNNVD-202101-538	1.250	5.000	0.385
		CNNVD-202101-792	1.333	4.000	0.308
		CNNVD-202101-820	3.000	3.000	0.231
		CNNVD-202102-678		1	0.077
	合计			13	1
3	资产使用率	CNNVD-202101-538	1.500	3.000	0.3
		CNNVD-202101-792	0.500	2.000	0.2
		CNNVD-202101-820	4.000	4.000	0.4
		CNNVD-202102-678		1	0.1
	合计			10	1
4	利益相关者风险承受度	CNNVD-202101-538	1.000	0.200	0.1
		CNNVD-202101-792	0.333	0.200	0.1
		CNNVD-202101-820	0.600	0.600	0.3
		CNNVD-202102-678		1	0.5
	合计			2	1
5	CVSS 基础组评分	CNNVD-202101-538	0.423	0.600	0.125
		CNNVD-202101-792	0.796	1.418	0.295
		CNNVD-202101-820	1.782	1.782	0.371
		CNNVD-202102-678		1	0.208
	合计			4.8	1

根据公式(7),计算漏洞危害消控优先级排序指 数 V_j,如表 6 所示。

表 6 漏洞危害消控优先级排序指数

Y	信息资产等级保护	网络防护与联通性	资产使用率	利益相关者风险承受度	CVSS 基础组评分	V_j
	0.3	0.3	0.2	0.1	0.1	
CNNVD-202101-538	0.2	0.385	0.3	0.1	0.125	0.257 885
CNNVD-202101-792	0.3	0.308	0.2	0.1	0.295	0.261 853
CNNVD-202101-820	0.1	0.231	0.4	0.3	0.371	0.246 352
CNNVD-202102-678	0.4	0.077	0.1	0.5	0.208	0.233 910

从表 6 可以看出,最先应关注的漏洞是 CNNVD-202101-792(高危);CNNVD-202101-820(超危)漏洞由于等保定级仅为一级,且在复杂保护的互联网访问之下等因素,是较为不受关注的漏洞;CNNVD-202102-678(中危)漏洞,由于处于物理隔离的网络环境中,虽然等保定级也较高,但使用人数较少同时利益相关者风险承受度较高,所以排在最后处理的位置;CNNVD-202101-538(低危)漏洞由于处于无保护的互联网环境之下、使用人数较多,利益相关者风险承受度也比较低等因素,反而成为需要给予较多关注的漏洞。这一漏洞风险评价结果,比单纯使用 NVD 给出的 CVSS 基础组评分或 CNNVD 给出的漏洞技术分级更为客观。

3　统计分析

3.1　相同环境指标的评分

本节收集了 2021 年 1 月开始 CNNVD 发布的 100 条公开漏洞,使用与评价示例中漏洞评价因素相同的初始权重,假设信息资产等级保护等级为三级,网络防护与联通性是复杂保护的互联网访问,具有 80% 的资产使用率,利益相关者风险承受度低。在此环境指标基础上,CNNVD 100 条公开漏洞 CVSS 静态分值变化,如图 1 中浅色曲线。MVSS 计算得出的漏洞危害消控优先级排序指数曲线,如图 1 中深色曲线。可以看出两条曲线区别仅在于波动振幅,峰谷波动趋势相同。在相同环境指标下 CVSS 基础组评分与 MVSS 评分漏洞数量分布上完全一致,如图 2 所示。

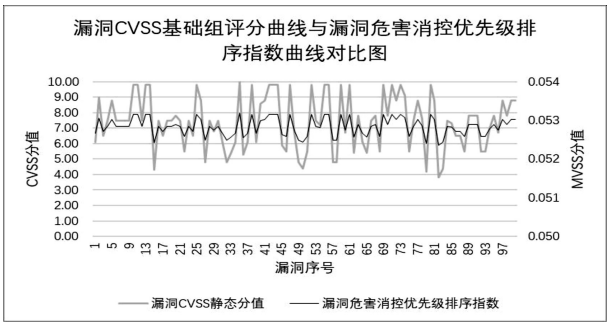

图 1　CVSS 与 MVSS 曲线对比

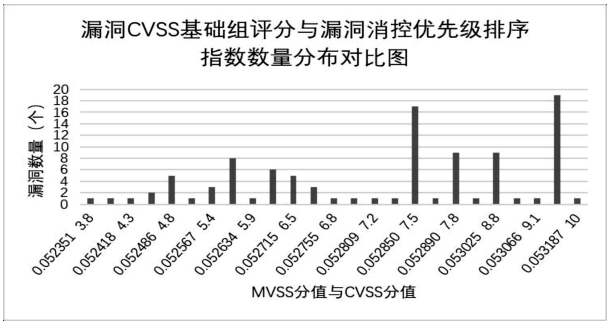

图 2　CVSS 与 MVSS 数量分布对比

上述两项统计分析说明,MVSS 评价方法本身不会改变漏洞固有 CVSS 基础组评分的相对位置,在同一系统中安全防护人员首先应关注的还是 CVSS 基础组评分较高的漏洞,这一点符合漏洞防护的基本规律。

3.2　不同环境指标的评分

本节选取了 CNNVD 不同 CVSS 静态分值的漏洞 22 个,分别以降序和升序的顺序排列,计算出环境因素风险等级由高到低情况下的 MVSS 分值。环境风险指标与漏洞 CVSS 静态分值对比,如图 3 所示。

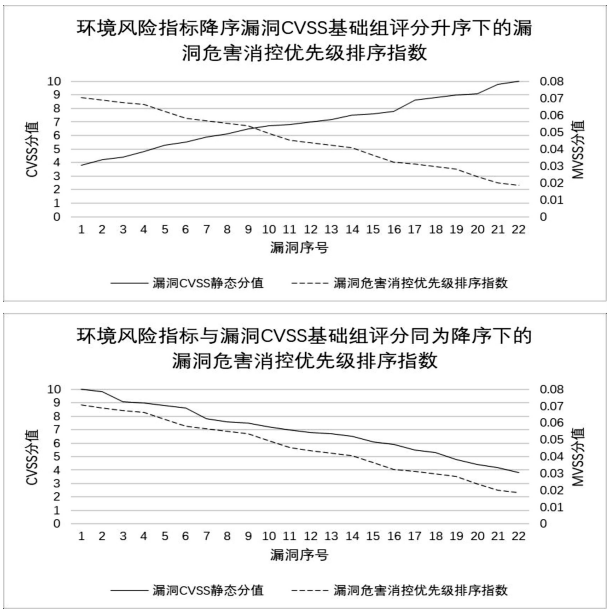

图 3　环境风险指标与漏洞 CVSS 基础组评分对比

可以看出,漏洞 CVSS 基础组评分与环境因素指标同为降序情况下,MVSS 评分与 CVSS 基础组评分走势相同;漏洞 CVSS 基础组评分与环境因素指标排序方式相反时,MVSS 评分与 CVSS 基础组评分也相反,此时 MVSS 给出的漏洞危害消控优先级排序结果显示,更应关注的是高风险环境下的 CVSS 基础组评分较低的漏洞。

4　结束语

该文给出的多因素漏洞评价方法,是将计算机系统分级评价、网络防护与联通性、资产使用率、利益相关者风险承受度和漏洞技术评价指标综合纳入量化评估范围。通过算法生成的 MVSS 指数可供信息系统运营者和安全技术人员评判漏洞消控优先级。选取 CNNVD-202101-538、CNNVD-202101-792、CNNVD-202101-820、CNNVD-202102-678 四条漏洞,以 CVSS 基础组评分为基础进行分析,展现了 MVSS 方法计算的全过程。并对 2021 年 CNNVD 发布的 100 条漏洞在不同环境因素下的情况进行了统计分析。分析结果表明,CVSS 评分体系适用于对漏洞开展技术研究、厂商漏洞定级、公众漏洞库漏洞批露等领域,MVSS 评分方法则更加侧重于信息系统运营者在开展漏洞消控工作中的漏洞评级,系统运营者和安

全技术人员使用 MVSS 方法可得出漏洞在实际环境中诸多因素影响下量化后的危害评估结果,对信息安全漏洞管理工作提供辅助决策依据。

参考文献:

[1] 《保密科学技术》编辑部. 2020 年网络安全事件盘点之国内篇[J]. 保密科学技术,2020(12):3-5.

[2] 《保密科学技术》编辑部. 2020 年网络安全事件盘点之国际篇[J]. 保密科学技术,2020(12):6-7.

[3] International Telecommunication Union. ITU-TX. 1521, Common Vulnerability Scoring System[S/OL]. (2016-03-23). https://www. itu. int/rec/T-REC-X. 1521-201603-I/en.

[4] Cybersecurity andInfrastructure Security Agency. National vulnerability database [S/OL]. 2018. https://nvd. nist. gov/.

[5] 中国国家标准化管理委员会. GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南[S]. 北京:中国标准出版社,2020.

[6] 中国信息安全测评中心. 中国国家信息安全漏洞库(China National Vulnerability Database of information security, CNNVD)[EB/OL]. 2009. http://www. cnnvd. org. cn/.

[7] Sandia National Laboratories. Methodology for prioritizing cybervulnerable critical infrastructure equipment and mitigation strategies[R/OL]. 2010. http://prod. sandia. gov/techlib/access-control. cgi/2010/101845. pdf.

[8] DAWSON L, MICHALSKI J, WYSS G, et al. IAEA-CN-228-56 Methodology for prioritizing cyber-vulnerable assets in nuclear power representative system architecture[R/OL]. 2015. https://www. osti. gov/servlets/purl/1258208.

[9] Gartner, Inc. Ganter site[EB/OL]. 2021. https://www. gartner. com/en.

[10] BARROS A, CHUVAKIN A. A guidance framework for developing and implementing vulnerability management [R/OL]. (2017-06-22). https://www. gartner. com/en/documents/3747620/a-guidance-framework-for-developing-and-implementing-vul.

[11] BARROS A, BELAK A, CLARK M. A guidance framework for developing and implementing vulnerability management [R/OL]. (2019-10-23). https://www. gartner. com/en/documents/3970669/a-guidance-framework-for-developing-and-implementing-vul.

[12] SPRING J, HATLEBACK E, HOUSEHOLDER A, et al. Prioritizing vulnerability response: a stakeholder-specific vulnerability categorization [R]. Carnegie Mellon University, 2019.

[13] SPRING J, HOUSEHOLDER A D, HATLEBACK E, et al. Prioritizing vulnerability response: a stakeholder-specific vulnerability categorization (version 2.0)[R]. Carnegie Mellon University, 2021.

[14] PETERSON D. ICS-patch what to patch when in ICS? a decision tree approach version 0.5[EB/OL]. 2020. https://www. linkedin. com/pulse/ics-patch-what-patch-when-dale-peterson.

[15] 黄家辉,冯冬芹,王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报,2016,42(5):792-798.

[16] 中国国家标准化管理委员会. GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求[S]. 北京:中国标准出版社,2019.

[17] Wikipedia Contributors. Trusted computer system evaluation criteria. Wikipedia, the free encyclopedia[EB/OL]. 2021. https://en. wikipedia. org/wiki/Trusted_Computer_System_Evaluation_Criteria#cite_note-2.

[18] U. S. Department of Defense. Department of defense instruction number 8500. 01[EB/OL]. 2014-03-14. https://www. esd. whs. mil/portals/54/documents/dd/issuances/dodi/850001_2014. pdf.

[19] ISO/IEC JTC 1/SC 27 IT Security techniques. ISO/IEC 15408-1:2009, information technology — security techniques — evaluation criteria for IT security — part 1: introduction and general model[S/OL]. 2014. https://www. iso. org/standard/50341. html.

[20] ISO/IEC JTC1/SC 27 IT Security techniques. ISO/IEC 15408-2:2008 information technology — security techniques — evaluation criteria for IT security — part 2: security functional components[S/OL]. 2011. https://www. iso. org/obp/ui/#iso:std:iso-iec:15408:-2:ed-3:v2:en.

[21] ISO/IEC JTC1/SC 27 IT Security techniques. ISO/IEC 15408-3:2008 information technology — security techniques — evaluation criteria for IT security — part 3: security assurance components[S/OL]. 2011. https://www. iso. org/obp/ui/#iso:std:iso-iec:15408:-3:ed-3:v2:en.