北京师范大学网络信息安全通告

2018 年 10 月报告

北京师范大学信息网络中心

2018 年 11 月

目录

漏洞态势 3
1. 公开漏洞情况 4
1.1. 漏洞增长概况 4
1.2. 漏洞分布情况 4
1.2.1. 漏洞厂商分布 4
1.2.2. 漏洞产品分布 5
1.2.3. 漏洞类型分布 6
1.2.4. 漏洞危害等级分布 7
1.3. 漏洞修复情况 7
1.3.1. 整体修复情况 7
1.3.2. 厂商修复情况 8
1.4. 重要漏洞实例 9
1.4.1. 超危漏洞实例 9
1.4.2. 高危漏洞实例 10
2. 接报漏洞情况 18
3. 重大漏洞预警 20
3.1.CNNVD 关于 Oracle WebLogic Server 远程代码执行漏洞的通报 20
3.2. CNNVD 关于微软多个安全漏洞的通报 21

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2018 年 10 月份采集安全漏洞共 1495 个。本月接报漏洞共计 2066 个，其中信息技术产品漏洞（通用型漏洞）62 个，网络信息系统漏洞（事件型漏洞）2004 个。

重大漏洞预警

1、Oracle WebLogic Server 远程代码执行漏洞（CNNVD-201810-781）：攻击者可利用该漏洞发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行。WebLogic Server 10.3.6.0、12.1.3.0、12.2.1.2、12.2.1.3 等版本均受漏洞影响。目前， Oracle 官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

2、微软官方发布了多个安全漏洞的公告，包括 Microsoft XML Core Services MSXML parsera 安全漏洞（CNNVD-201810-294）、Microsoft Windows Hyper-V 安全漏洞（CNNVD-201810-327）等多个漏洞。成功利用上述漏洞的攻击者，可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已发布修复上述漏洞的补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

1. 公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2018 年 10 月新增安全漏洞共 1495 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 183 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 12.31%。本月新增漏洞中，超危漏洞 17 个、高危漏洞 254 个、中危漏洞 999 个、低危漏洞 225 个，相应修复率分别为 82.35%、90.55%、74.67%以及 66.67%。合计 1140 个漏洞已有修复补丁发布，本月整体修复率为 76.25%。截至 2018 年 10 月 31 日，CNNVD 采集漏洞总量已达 117293 个。

1.1. 漏洞增长概况

2018 年 10 月新增安全漏洞 1495 个，与上月（1324 个）相比增加了 12.92%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1374 个。

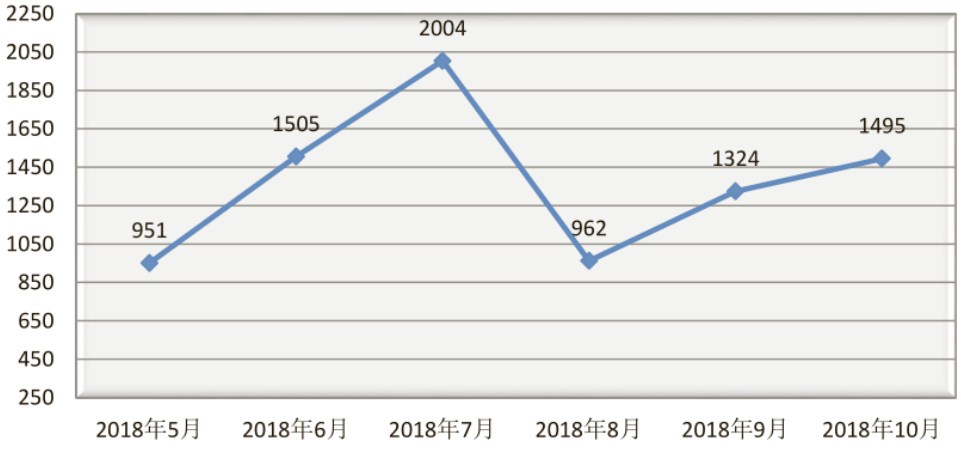

图 1 2018 年 5 月至 2018 年 10 月漏洞新增数量统计图

1.2. 漏洞分布情况

1.2.1. 漏洞厂商分布

10 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司达到 183 个，占本月漏洞总量的 12.24%。

表1　2018 年9 月新增安全漏洞排名前十厂商统计表

序号	厂商名称	漏洞数量	所占比例
1	Oracle	183	12.24%
2	福昕	128	8.56%
3	Adobe	102	6.82%
4	IBM	69	4.62%
5	思科	66	4.41%
6	Qualcomm	61	4.08%
7	微软	49	3.28%
8	谷歌	46	3.08%
9	Juniper Networks	21	1.40%
10	Mozilla	17	1.14%

1.2.2. 漏洞产品分布

10 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 33 条，其中桌面操作系统 33 条，服务器操作系统 29 条。本月 Windows 10 漏洞数量最多，达到 33 个，占主流操作系统漏洞总量的 16.67%，排名第一。

表 2　2018 年 10 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Windows 10	33
2	Windows Server 2016	26
3	Android	26
4	Windows Server 1709	20
5	Windows Server 2012	17
6	Windows 8.1	16
7	Windows Rt 8.1	16

8	Windows Server 2008	16
9	Windows 7	14
10	Linux Kernel	11
11	Apple iOS	3

说明：

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计。

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3. 漏洞类型分布

10 月发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 12.38%。

表3　2018 年 10 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	跨站脚本	185	12.38%
2	缓冲区错误	170	11.37%
3	信息泄露	47	3.15%
4	SQL 注入	37	2.48%
5	输入验证	35	2.34%
6	权限许可和访问控制	28	1.87%
7	跨站请求伪造	27	1.81%
8	访问控制错误	19	1.27%
9	路径遍历	14	0.94%
10	数字错误	12	0.81%
11	资源管理错误	10	0.67%
12	操作系统命令注入	7	0.47%

13	命令注入	4	0.27%
14	授权问题	3	0.20%
15	代码注入	1	0.07%
16	竞争条件	1	0.07%
17	配置错误	1	0.07%
18	信任管理	1	0.07%

1.2.4. 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。10 月漏洞危害等级分布如图 2 所示，其中超危漏洞 17 条，占本月漏洞总数的 1.49%。

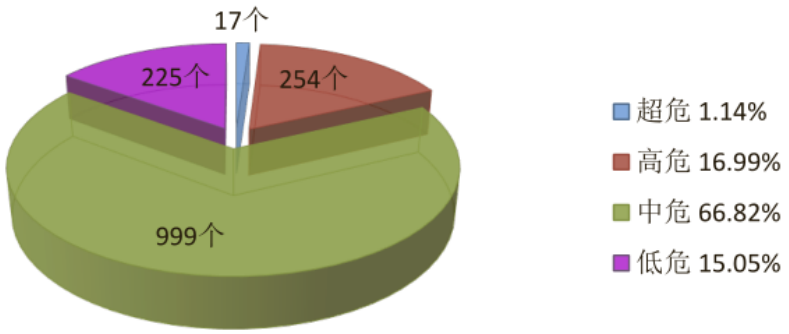

图 2　2018 年 10 月漏洞危害等级分布

1.3. 漏洞修复情况

1.3.1. 整体修复情况

10 月漏洞修复情况按危害等级进行统计见图 3。其中高危漏洞修复率最高，达到 90.55%，低危漏洞修复率最低，比例为 66.67%。与上月相比，本月高危漏洞修复率有所上升，超危、中危、低危漏洞修复率有所下降。总体来看，本月漏洞整体修复率上升，由上月的 68.71%上升至本月的 76.25%。

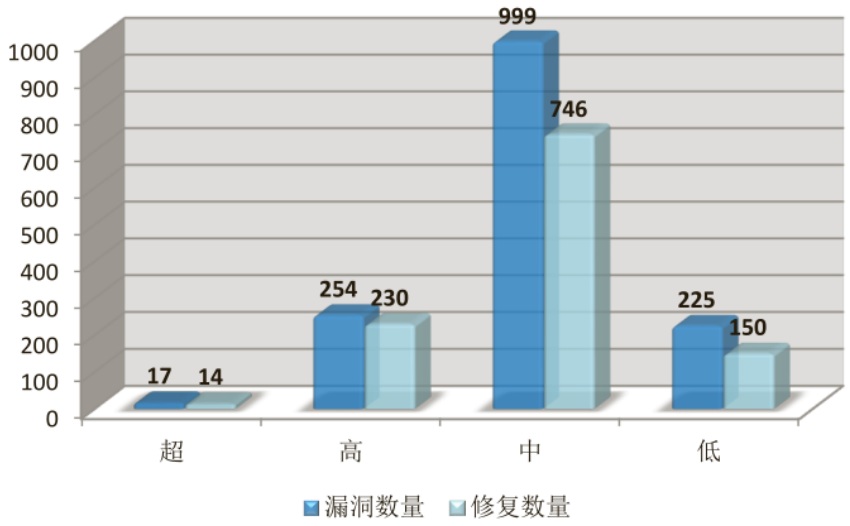

图 3　2018 年 10 月漏洞修复数量统计

1.3.2. 厂商修复情况

10 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、福昕、Adobe 等十个厂商共 742 条漏洞，占本月漏洞总数的 49.63%，漏洞修复率为 99.33%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Oracle、福昕、Adobe、IBM、Qualcomm、微软、Juniper Networks、Mozilla、Dell、Apache 等公司本月漏洞修复率均为 100%，共 824 条漏洞已全部修复。

表4　　2018 年10 月厂商修复情况统计表

序号	厂商名称	漏洞数量	修复数量	修复率
1	Oracle	183	183	100.00%
2	福昕	128	128	100.00%
3	Adobe	102	102	100.00%
4	IBM	69	69	100.00%
5	思科	66	64	96.97%
6	Qualcomm	61	61	100.00%
7	微软	49	49	100.00%
8	谷歌	46	43	93.48%
9	Juniper Networks	21	21	100.00%

10	Mozilla	17	17	100.00%

1.4. 重要漏洞实例

1.4.1. 超危漏洞实例

10 月超危漏洞共 17 个，其中重要漏洞实例如表 5 所示。

表 5 2018 年 10 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	权限许可和访问控制	CNNVD-201810-062	谷歌	Android 权限许可和访问控制漏洞（CNNVD-201810-062）
2	缓冲区错误	CNNVD-201810-727	NEOJAPAN	NEOJAPAN Denbun POP 和 Denbun IMAP 缓冲区错误漏洞（CNNVD-201810-727）

1. Android 权限许可和访问控制漏洞（CNNVD-201810-062）

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。

Android 8.0 版本和 8.1 版本中的 avrc_pars_tg.cc 文件的‘avrc_pars_browsing_cmd’函数存在提权漏洞。远程攻击者可通过发送特制的参数利用该漏洞在系统上获取提升的权限。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2018-10-01

2. NEOJAPAN Denbun POP NEOJAPAN Denbun POP 和 Denbun IMAP （CNNVD-201810-727）

NEOJAPAN Denbun POP 和 Denbun IMAP 都是日本 NEOJAPAN 公司的基于 Web 的电子邮件系统。NEOJAPAN Denbun POP 是它的支持 POP 协议的版本；Denbun IMAP 是支持 IMAP 协议的版本。

NEOJAPAN Denbun POP 3.3P R4.0 及之前版本和 Denbun IMAP3.3I R4.0 及之前版本中存在基于栈的缓冲区溢出漏洞。远程攻击者可利用该漏洞执行任意代码或造应用程序崩溃。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://denbun.com/ja/imap/support/security/181003.html

1.4.2. 高危漏洞实例

本月高危漏洞共 254 个，其中重点漏洞实例如表 6 所示。

表 6 2018 年 10 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	信任管理	CNNVD-201810-184	思科	Cisco Prime Collaboration Provisioning 信任管理漏洞（CNNVD-201810-184）
2	信息泄露	CNNVD-201810-066 CNNVD-201810-070 CNNVD-201810-072 CNNVD-201810-073 CNNVD-201810-075 CNNVD-201810-076 CNNVD-201810-077 CNNVD-201810-078 CNNVD-201810-079 CNNVD-201810-080	谷歌	Android download manager 信息泄露漏洞（CNNVD-201810-066）
3	数字错误	CNNVD-201810-403 CNNVD-201810-404	Adobe	Adobe Acrobat 和Reader 数字错误漏洞（CNNVD-201810-403）

4	权限许可和访问控制	CNNVD-201810-065 CNNVD-201810-071 CNNVD-201810-082 CNNVD-201810-083 CNNVD-201810-084	谷歌	Microsoft Windows Kernel权限许可和访问控制漏洞（CNNVD-201810-329）
		CNNVD-201810-306	微软	
		CNNVD-201810-329		
5	缓冲区错误	CNNVD-201810-973	Oracle	Oracle GoldenGate 缓冲区错误漏洞（CNNVD-201810-973）
		CNNVD-201810-355	Mozilla	
		CNNVD-201810-405 CNNVD-201810-406 CNNVD-201810-407 CNNVD-201810-408 CNNVD-201810-409 CNNVD-201810-410 CNNVD-201810-411 CNNVD-201810-412 CNNVD-201810-413 CNNVD-201810-414 CNNVD-201810-416 CNNVD-201810-417 CNNVD-201810-418 CNNVD-201810-419 CNNVD-201810-420 CNNVD-201810-421 CNNVD-201810-422 CNNVD-201810-423 CNNVD-201810-424 CNNVD-201810-425 CNNVD-201810-426 CNNVD-201810-427 CNNVD-201810-428 CNNVD-201810-429 CNNVD-201810-430 CNNVD-201810-431 CNNVD-201810-432 CNNVD-201810-433 CNNVD-201810-434 CNNVD-201810-435	Adobe	

		CNNVD-201810-436 CNNVD-201810-437 CNNVD-201810-438		
		CNNVD-201810-571 CNNVD-201810-573 CNNVD-201810-575 CNNVD-201810-599 CNNVD-201810-605	福昕	
		CNNVD-201810-1273	研华	
6	访问控制错误	CNNVD-201810-190	思科	SaltStack Salt 访问控制错误漏洞（CNNVD-201810-1235）
		CNNVD-201810-1235	SaltStack	
		CNNVD-201810-1272	研华	
7	资源管理错误	CNNVD-201810-186	思科	Cisco Remote PHY Software资源管理错误漏洞（CNNVD-201810-186）
8	输入验证	CNNVD-201810-183	思科	Cisco SD-WAN Solution 输入验证漏洞（CNNVD-201810-183）
9	配置错误	CNNVD-201810-182	思科	Cisco Digital Network Architecture Center 配置错误漏洞（CNNVD-201810-182）

1. Cisco Prime Collaboration Provisioning 信任管理漏洞（CNNVD-201810-184）

Cisco Prime Collaboration Provisioning（PCP）是美国思科（Cisco）公司的一套基于 Web 的下一代通信服务软件。该软件对 IP 电话、语音邮件和统一通信环境提供 IP 通信服务功能。

Cisco PCP 12.1 之前版本中的安装功能存在信任管理漏洞。远程攻击者可借助默认的硬编码用户名和密码利用该漏洞以管理员级别权限访问管理 Web 界面。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-cpcp-password

2. Android download manager 信息泄露漏洞（ CNNVD-201810-066 ）

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。DownloadManager 是其中的一个下载管理器。

Android 中的 download manager 的 content provider 存在信息泄露漏洞，该漏洞源于程序没有执行正确的输入验证。本地攻击者可通过发送特制的请求利用该漏洞获取敏感信息。以下版本受到影响：

- Android 7.0 版本
- Android 7.1.1 版本
- Android 7.1.2 版本
- Android 8.0 版本
- Android 8.1 版本
- Android 9 版本

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2018-10-01

3. Adobe Acrobat 和 Reader 数字错误漏洞（CNNVD-201810-403）

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。前者是一套 PDF 文件编辑和转换工具，后者是一套 PDF 文档阅读软件。

Adobe Acrobat 和 Reader 中存在整数溢出漏洞。远程攻击者可利用该漏洞获取敏感信息。基于 Windows 和 macOS 平台的以下产品和版本受到影响：

-Adobe Acrobat DC（Continuous）2018.011.20063 及之前版本

-Adobe Acrobat 2017（Classic 2017）2017.011.30102 及之前版本

-Adobe Acrobat DC（Classic 2015）2015.006.30452 及之前版本

-Adobe Acrobat Reader DC（Continuous）2018.011.20063 及之前版本

-Adobe Acrobat Reader 2017（Classic 2017）2017.011.30102 及之前版本

-Adobe Acrobat Reader DC（Classic 2015）2015.006.30452 及之前版本

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html

4. Microsoft Windows Kernel 权限许可和访问控制漏洞（CNNVD-201810-329）

Microsoft Windows Server 2019 等都是美国微软（Microsoft）公司发布的一系列操作系统。Windows Kernel 是其中的一个 Windows 系统内核。

Microsoft Windows Kernel 中对内核内存处理的方式存在提权漏洞。本地攻击者可利用该漏洞以提升的权限执行任意代码。以下系统版本受到影响：

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 版本 1803
- Microsoft Windows Server 版本 1709
- Microsoft Windows 10 版本 1809
- Microsoft Windows 10 版本 1803
- Microsoft Windows 10 版本 1709
- Microsoft Windows 10 版本 1703
- Microsoft Windows 10 版本 1607

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8497

5. Oracle GoldenGate 缓冲区错误漏洞（CNNVD-201810-973）

Oracle GoldenGate 是美国甲骨文（Oracle）公司一个用于在 IT 环境中进行实时数据集成和复制的综合软件包，它支持实时数据集成、事务型变更数据捕获、数据服务、转换和验证功能。

Oracle GoldenGate 12.1.2.1.0 版本、12.2.0.2.0 版本和 12.3.0.1.0 版本中的 Monitoring Manager 子组件存在安全漏洞。攻击者可利用该漏洞控制组件，影响数据的可用性、保密性和完整性。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html

6. SaltStack Salt 访问控制错误漏洞（CNNVD-201810-1235）

SaltStack Salt（又名 SaltStack）是美国 SaltStack 公司的一套开源的用于管理基础架构的工具。该工具提供配置管理、远程执行等功能，能够管理上万台服务器，具有快速完成数据传递的能力。

SaltStack Salt 2017.7.8 之前版本和 2018.3.3 之前的 2018.3.x 版本中存在访问控制错误漏洞。远程攻击者可借助 salt-api（netapi）利用该漏洞绕过身份验证，执行任意命令。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.saltstack.com/en/latest/topics/releases/2018.3.3.html

7. Cisco Remote PHY Software 资源管理错误漏洞（CNNVD-201810-186）

Cisco Remote PHY Software 是美国思科（Cisco）公司的一套基于数字光纤的 DOCSIS 解决方案。该方案使用以太网 PON（EPON）和城域网络等作为传输网络。

Cisco Remote PHY Software 中的 IPv4 碎片处理函数存在资源管理错误漏洞。远程攻击者可通过发送畸形的流量利用该漏洞造成拒绝服务。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-phy-ipv4-dos

8. Cisco SD-WAN Solution 输入验证漏洞（CNNVD-201810-183）

Cisco vEdge 100 Series Routers 等都是美国思科（Cisco）公司的不同系列的路由器产品。SD-WAN Solution 是运行在其中的一套网络扩展解决方案。

Cisco SD-WAN Solution 17.2.8 之前版本和 18.3.1 之前版本中存在输入验证漏洞，该漏洞源于程序没有正确的验证证书。远程攻击者可通过向受影响的设备提交使用特制证书所签名的系统镜像利用该漏洞绕过证书检测，部署特制的系统镜像。以下产品受到影响：

- Cisco vBond Orchestrator Software
- Cisco vEdge 100 Series Routers
- Cisco vEdge 1000 Series Routers
- Cisco vEdge 2000 Series Routers
- Cisco vEdge 5000 Series Routers
- Cisco vEdge Cloud Router Platform
- Cisco vManage Network Management Software
- Cisco vSmart Controller Software

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-sd-wan-bypass

9. Cisco Digital Network Architecture Center 配置错误漏洞（CNNVD-201810-182）

Cisco Digital Network Architecture Center（DNA Center）是美国思科（Cisco）公司的一套数字网络体系结构解决方案。该方案能够扩展并保护网络内的设备、应用程序等。

Cisco DNA Center 1.1 版本中存在配置错误漏洞，该漏洞源于受影响系统中带有不安全的默认配置。远程攻击者可利用该漏洞检索和修改重要的系统文件。

解决措施：目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181003-dna-unauth-access

2. 接报漏洞情况

本月接报漏洞共计 2066 个，其中信息技术产品漏洞（通用型漏洞）62 个，网络信息系统漏洞（事件型漏洞）2004 个。

表 7 2018 年 10 月漏洞接报情况

序号	报送单位	漏洞总量	通用型漏洞	事件型漏洞
1	网神信息技术（北京）股份有限公司	844	0	844
2	上海斗象信息科技有限公司	717	0	717
3	北京数字观星科技有限公司	185	0	185
4	中新网络信息安全股份有限公司	141	2	139
5	内蒙古奥创科技有限公司	55	15	40
6	四川虹微技术有限公司	31	0	31
7	广州锦行网络科技有限公司	19	4	15
8	国发中新（北京）科技发展有限公司	18	0	18
9	深圳爱加密科技有限公司	15	15	0
10	任子行信息技术有限公司	14	0	14
11	北京山石网科信息技术有限公司	9	9	0
12	北京天融信网络安全技术有限公司	5	5	0
13	北京威努特技术有限公司	4	4	0
14	个人报送	2	2	0

15	杭州海康威视数字技术股份有限公司	2	2	0
16	北京邮电大学	1	1	0
17	国防科技大学	1	1	0
18	海南大学	1	0	1
19	江苏博智软件科技股份有限公司	1	1	0
20	沈阳汉林科技有限公司安全服务部	1	1	0
报送总计		2066	62	2004

3. 重大漏洞预警

3.1. CNNVD 关于 Oracle WebLogic Server 远程代码执行漏洞的通报

本月，国家信息安全漏洞库（CNNVD）收到 Oracle WebLogicServer 远程代码执行漏洞（CNNVD-201810-781、CVE-2018-3245）情况的报送。攻击者可利用该漏洞发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作，最终实现远程代码执行。WebLogic Server 10.3.6.0、12.1.3.0、12.2.1.2、12.2.1.3 等版本均受漏洞影响。目前，Oracle 官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

Oracle WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

Oracle WebLogic Server 存在远程代码执行漏洞（CNNVD-201810-781、CVE-2018-3245）。该漏洞通过 JRMP 协议利用 RMI 机制的缺陷达到远程代码执行的目的。攻击者可以在未授权的情况下将 payload 封装在 T3 协议中，通过对 T3 协议中的 payload 进行反序列化，从而实现对存在漏洞的 WebLogic 组件进行远程攻击，执行任意代码，并获取目标系统的所有权限。

漏洞危害

攻击者可利用漏洞在未授权的情况下发送攻击数据，通过 T3 协议在 WebLogic Server 中执行反序列化操作,最终实现远程代码执行。该漏洞涉及了多个版本，具体受影响版本如下：

- Oracle WebLogic Server 10.3.6.0
- Oracle WebLogic Server 12.1.3.0
- Oracle WebLogic Server 12.2.1.2

- Oracle WebLogic Server 12.2.1.3

修复措施

目前，Oracle 官方已经发布补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

（1）Oracle 官方更新链接如下：

https://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html

（2）临时解决方案：

通过设置 weblogic.security.net.ConnectionFilterImpl 默认连接筛选器，对 T3/T3s 协议的访问权限进行配置，阻断漏洞利用途径。具体如下：

（a）进入 WebLogic 控制台，在 base_domain 的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

（b）在连接筛选器中输入：WebLogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：** 7001 deny t3 t3s

（c）保存后重新启动即可生效。

3.2. CNNVD 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 MS XML 远程执行代码漏洞（CNNVD-201810-294、CVE-2018-8494）、Windows Hyper-V 远程执行代码漏洞（CNNVD-201810-327、CVE-2018-8490）等多个漏洞。成功利用上述安全漏洞的攻击者，可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞介绍

本次漏洞通报涉及 Microsoft Edge、Internet Explorer、Microsoft 脚本引擎、Windows Hyper-V、Chakra 脚本引擎等 Windows 平台下应用软件和组件。漏洞详情如下：

1、 Internet Explorer 内存损坏漏洞（CNNVD-201810-297、CVE-2018-8491）、（CNNVD-201810-300、CVE-2018-8460）

漏洞简介：Internet Explorer 部分版本存在远程代码执行漏洞，当 Internet Explorer 不正确地访问内存中的对象时，可触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。

2、 Microsoft Edge 内存损坏漏洞（CNNVD-201810-292、CVE-2018-8473）、（CNNVD-201810-302、CVE-2018-8509）

漏洞简介：当 Microsoft Edge 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。

3、 Microsoft Edge 内存损坏漏洞（CNNVD-201810-327、CVE-2018-8490）、（CNNVD-201810-328、CVE-2018-8489）

漏洞简介：当主机服务器上的 Windows Hyper-V 无法正确验证用户操作系统上经身份验证的用户的输入时，存在远程代码执行会触发该漏洞。成功利用此漏洞的攻击者可以执行任意代码。

4、 Chakra 脚本引擎内存损坏漏洞（CNNVD-201810-303、CVE-2018-8500）、（CNNVD-201810-307、CVE-2018-8505）、（CNNVD-201810-309、CVE-2018-8511）、（CNNVD-201810-310、CVE-2018-8510）、（CNNVD-201810-334、CVE-2018-8513）

漏洞简介：Chakra 脚本引擎在 Microsoft Edge 中处理内存中的对象的方式中时存在远程代码执行可能触发漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，攻击者便可以控制受影响的系统。攻击者可任意安装程序、查看、更改或删除数据、或者创建新帐户。

5、 MS XML 远程执行代码漏洞（CNNVD-201810-294、CVE-2018-8494）

漏洞简介：当 Microsoft XML Core Services MSXML 分析器处理用户输入时，存在代码远程执可能触发该行漏洞。成功利用此漏洞的攻击者可以远程运行恶意代码控制用户的系统。

安全建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方链接地址如下：

1. Internet Explorer 内存损坏漏洞（CNNVD-201810-297、CVE-2018-8491）、（CNNVD-201810-300、CVE-2018-8460）修复补丁链接地址：

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8491

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8460

2. Microsoft Edge 内存损坏漏洞（CNNVD-201810-292、CVE-2018-8473）、（CNNVD-201810-302、CVE-2018-8509）修复补丁链接地址：

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8473

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8509

3. Windows Hyper-V 远程执行代码漏洞（CNNVD-201810-327、CVE-2018-8490）、（CNNVD-201810-328、CVE-2018-8489）修复补丁链接地址：

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8490

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8489

4. Chakra 脚本引擎内存损坏漏洞（CNNVD-201810-303、CVE-2018-8500）、（CNNVD-201810-307、CVE-2018-8505）、（CNNVD-201810-309、CVE-

2018-8511）、（CNNVD-201810-310、CVE-2018-8510）、（CNNVD-201810-334、CVE-2018-8513）修复补丁链接地址：

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8500

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8505

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8511

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8510

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8513

5. MS XML 远程执行代码漏洞（CNNVD-201810-294、CVE-2018-8494）修复补丁链接地址：

https://portal.msrc.microsoft.com/zh-cn/security-guidance/advisory/CVE-2018-8494