信息安全漏洞周报

（2020 年第 5 期 总第 509 期）

信息安全测评中心　　2020 年 2 月 9 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 2 月 3 日至 2020 年 2 月 9 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 260 个，与上期（496 个）相比减少了了 47.58%。

接报漏洞情况

本周 CNNVD 接报漏洞 268 个，其中信息技术产品漏洞（通用型漏洞）0 个，网络信息系统漏洞（事件型漏洞）268 个。

接报漏洞情况

思科 CDP 设备多个安全漏洞预警：包括思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、CVE-2020-3111）。成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。目前，思科官方已发布漏洞补丁修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 260 个，漏洞新增数量有所下降。从厂商分布来看 Nextcloud 公司新增漏洞最多，有 21 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 14.62%。新增漏洞中，新增漏洞中，超危漏洞 31 个，高危漏洞 80 个，中危漏洞 139 个，低危漏洞 10 个。相应修复率分别为 77.42%、87.50%、73.38%和 80.00%。根据补丁信息统计，合计 204 个漏洞已有修复补丁发布，整体修复率为 78.46%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 260 个，与上周（496 个）相比降低了 47.58%。图 1 为近六周漏洞新增数量统计图。

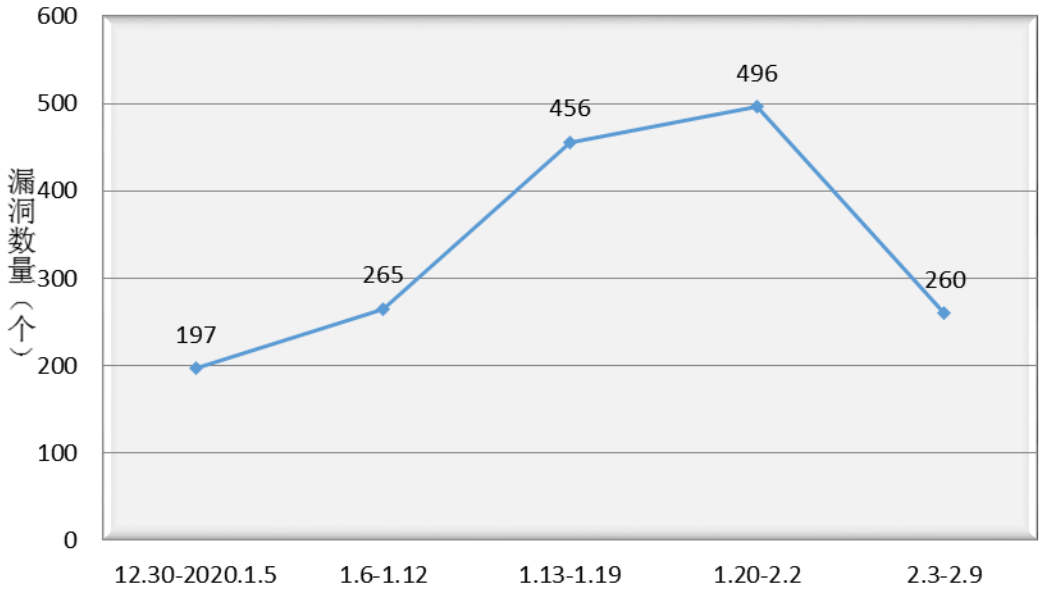

图 1 近六周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Nextcloud 公司新增漏洞最多，有 21 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量（个）	所占比例
1	Nextcloud	21	8.07%
2	IBM	15	5.76%
3	GitLab	14	5.38%
4	Qualcomm	11	4.23%
5	Atlassian	9	3.46%

2020 年 2 月 3 日至 2020 年 2 月 9 日，国内厂商漏洞 6 个，友讯公司漏洞数量最多，有 5 个。国内厂商漏洞整体修复率为 100.00%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看,跨站脚本类的安全漏洞占比最大，达到 14.62%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	跨站脚本	38	14.62%
2	输入验证错误	23	8.85%
3	信息泄露	21	8.08%
4	资源管理错误	15	5.77%
5	缓冲区错误	15	5.77%
6	授权问题	12	4.62%
7	代码问题	9	3.46%
8	跨站请求伪造	9	3.46%
9	SQL 注入	8	3.08%
10	路径遍历	8	3.08%
11	访问控制错误	5	1.92%
12	操作系统命令注入	3	1.15%
13	注入	2	0.77%
14	数据伪造问题	1	0.38%
15	加密问题	1	0.38%
16	信任管理问题	1	0.38%
17	命令注入	1	0.38%
18	安全特征问题	1	0.38%

19	竞争条件问题	1	0.38%
20	环境问题	1	0.38%
21	格式化字符串错误	1	0.38%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 31 个，高危漏洞 80 个，中危漏洞 139 个，低危漏洞 10 个。相应修复率分别为 77.42%、87.50%、73.38%和 80.00%。根据补丁信息统计，合计 204 个漏洞已有修复补丁发布，整体修复率为 78.46%%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	31	24	77.42%
2	高危	80	70	87.50%
3	中危	139	102	73.38%
4	低危	10	8	80.00%
合计		260	204	78.46%

（四） 本周重要漏洞实例

本周重要漏洞实例如表 4 所示。

表 4 本周重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	输入验证错误	CNNVD-202002-201	Qualcomm	多款 Qualcomm 产品输入验证错误漏洞	是	超危
2	格式化字符串错误	CNNVD-202002-131	Cisco	Cisco IOS XR 格式化字符串错误漏洞	是	高危
3	加密问题	CNNVD-202002-043	IBM	IBM Security Directory Server 加密问题漏洞	是	高危

1. 多款 Qualcomm 产品输入验证错误漏洞（CNNVD-202002-201）

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司的产品。MDM9206 是一款中央处理器（CPU）产品。MDM9607 是一款中央处理器（CPU）产品。SDX20 是一款调制解调器。

多款 Qualcomm 产品中的 Video 存在输入验证错误漏洞。该漏洞源于网络系统或产品未对输入的数据进行正确的验证。以下产品及版本受到影响：

- Qualcomm APQ8009
- Qualcomm APQ8017
- Qualcomm APQ8053
- Qualcomm APQ8064
- Qualcomm APQ8096AU
- Qualcomm APQ8098
- Qualcomm MDM9206
- Qualcomm MDM9207C
- Qualcomm MDM9607
- Qualcomm MSM8905
- Qualcomm MSM8909W
- Qualcomm MSM8917
- Qualcomm MSM8920
- Qualcomm MSM8937
- Qualcomm MSM8939
- Qualcomm MSM8940

- Qualcomm MSM8953
- Qualcomm MSM8996
- Qualcomm MSM8996AU
- Qualcomm MSM8998
- Qualcomm Nicobar
- Qualcomm QCS405
- Qualcomm QCS605
- Qualcomm QM215
- Qualcomm Rennell
- Qualcomm SA6155P
- Qualcomm Saipan
- Qualcomm SDA660
- Qualcomm SDA845
- Qualcomm SDM429
- Qualcomm SDM429W
- Qualcomm SDM439
- Qualcomm SDM450
- Qualcomm SDM630
- Qualcomm SDM632
- Qualcomm SDM636
- Qualcomm SDM660
- Qualcomm SDM670

- Qualcomm SDM710
- Qualcomm SDM845
- Qualcomm SDX20
- Qualcomm SM6150
- Qualcomm SM7150
- Qualcomm SM8150
- Qualcomm SM8250
- Qualcomm SXR1130
- Qualcomm SXR2130

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.qualcomm.com/company/product-security/bulletins/february-2020-bulletin

2. Cisco IOS XR 格式化字符串错误漏洞（CNNVD-202002-131）

Cisco IOS XR 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XR Cisco Discovery Protocol 中存在格式化字符串错误漏洞。该漏洞源于网络系统或产品接收外部格式化字符串作为参数时，对参数类型、数量等过滤不严格。

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-20200205-iosxr-cdp-rce

3. IBM Security Directory Server 加密问题漏洞

（CNNVD-202002-043）

IBM Security Directory Server 是美国 IBM 公司的一套使用了轻量级目录访问协议（LDAP）的企业身份管理软件。该软件提供一个可信的身份数据基础架构，用于身份验证。

IBM Security Directory Server 中存在加密问题漏洞。该漏洞源于网络系统或产品未正确使用相关密码算法，导致内容未正确加密、弱加密、明文存储敏感信息等。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/1288660

二、接报漏洞情况

本周 CNNVD 接报漏洞 268 个，其中信息技术产品漏洞（通用型漏洞）0 个，网络信息系统漏洞（事件型漏洞）268 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	网神信息技术（北京）股份有限公司	101
2	上海斗象信息科技有限公司	96
3	内蒙古洞明科技有限公司	70
4	个人	1
报送总计		268

三、重大漏洞预警

思科 CDP 设备多个安全漏洞预警

近日，国家信息安全漏洞库（CNNVD）收到关于思科 CDP 设备多个安全漏洞情况的报送，包括思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、CVE-2020-3111）等多个漏洞。成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。思科 Firepower 1000 Series、IOS XRv 9000 Router、Nexus 1000V Switch、IP Conference Phone 7832、Video Surveillance 8000 Series IP Camera 等多款设备均受此漏洞影响。目前，思科官方已发布漏洞补丁修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

（一）漏洞介绍

思科公司是美国一家网络解决方案供应商，CDP 是思科（Cisco）专有的第二层（数据链路层）网络协议，主要用来对本地连接的思科设备进行信息获取。几乎所有的思科产品，包括交换机、路由器、IP 电话和摄像头等，都实现了 CDP 协议，且这些设备出厂时均默认启用 CDP。

1、思科视频监控 8000 系列 IP 摄像头 CDP 远程代码执行漏洞（CNNVD-202002-127、CVE-2020-3110）：

思科视频监控 8000 系列 IP 摄像头的 CDP 协议实现在解析数据包中的 DeviceID 字段时，存在堆溢出漏洞。通过利用此漏洞，攻击者可以对目标设备实施远程代码执行或拒绝服务攻击。

2、思科 VoIP 电话 CDP 远程代码执行漏洞（CNNVD-202002-128、

CVE-2020-3111）

思科 VoIP 电话的 CDP 协议实现在解析 CDP 数据包中的 PortID 字段时，存在栈溢出漏洞。通过利用此漏洞，攻击者可以对目标设备实施远程代码执行或拒绝服务攻击。

3、思科 IOS-XR CDP 格式化字符串漏洞（CNNVD-202002-131、CVE-2020-3118）

思科 IOS XR 的 CDP 协议实现，在解析 CDP 请求包中的某些字符串字段时（比如设备 ID、端口 ID 等），存在格式化字符串漏洞。通过利用此漏洞，攻击者可以在目标路由器上执行任意代码，获取系统权限。

4、思科 NX-OS CDP 远程代码执行漏洞（CNNVD-202002-130、CVE-2020-3119）

运行有思科 NX-OS 软件的设备的 CDP 协议实现，在解析含有 PoE（Power over Ethernet）请求字段的 CDP 数据包时，存在栈溢出漏洞。通过利用此漏洞，攻击者可以在目标交换机上执行任意代码，获取系统权限。

5、思科 FXOS、IOS XR、NX-OS CDP 拒绝服务漏洞（CNNVD-202002-129、CVE-2020-3120）

运行有思科 FXOS、IOS XR 或 NX-OS 软件的设备，其 CDP 协议实现存在拒绝服务漏洞。通过利用此漏洞，攻击者可以对运行有这些软件的目标设备进行拒绝服务攻击。

（二）危害影响

成功利用这些漏洞的攻击者，可以远程执行任意代码，获取系统权限。思科 Firepower 1000 Series、IOS XRv 9000 Router、Nexus 1000V Switch、IP Conference Phone 7832、Video Surveillance 8000 Series IP Camera 等多款设备均受此漏洞影响，具体如下：

序号	类型	型号
1	路由器	ASR 9000 Series Aggregation Services Routers Carrier Routing System (CRS) Firepower 1000 Series Firepower 2100 Series Firepower 4100 Series Firepower 9300 Security Appliances IOS XRv 9000 Router White box routers running Cisco IOS XR
2	交换机	Nexus 1000 Virtual Edge Nexus 1000V Switch Nexus 3000 Series Switches Nexus 5500 Series Switches Nexus 5600 Series Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Fabric Switches MDS 9000 Series Multilayer Switches Network Convergence System (NCS) 1000 Series Network Convergence System (NCS) 5000 Series Network Convergence System (NCS) 540 Routers

		Network Convergence System (NCS) 5500 Series Network Convergence System (NCS) 560 Routers Network Convergence System (NCS) 6000 Series UCS 6200 Series Fabric Interconnects UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects
3	IP 电话	IP Conference Phone 7832 IP Conference Phone 8832 IP Phone 6800 Series IP Phone 7800 Series IP Phone 8800 Series IP Phone 8851 Series Unified IP Conference Phone 8831 Wireless IP Phone 8821 Wireless IP Phone 8821-EX
4	IP 摄像头	Video Surveillance 8000 Series IP Cameras

（三）修复建议

目前，思科官方已发布漏洞补丁修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方补丁地址如下：

https://tools.cisco.com/security/center/publicationListing.x