安全事件通告

微软 Exchange 多个高危漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-03-03

报告信息

报告名称	微软 Exchange 多个高危漏洞通告		
报告类型	安全事件通告	**报告编号**	B6-2021-030301
报告版本	1	**报告日期**	2021-03-03
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-03-03	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	服务端请求伪造等
CVE 编号	CVE-2021-26855 等
相关厂商	Microsoft
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
事件发布时间	2021-03-03
报告生成时间	2021-03-03

二、事件简述

2021 年 03 月 03 日，360CERT 监测发现 微软 发布了 Exchange 多个高危漏洞的风险通告，该漏洞编号为 CVE-2021-26855,CVE-2021-26857,CVE-2021-26858,CVE-2021-27065 ，事件等级：严重，事件评分：9.8。

对此，360CERT 建议广大用户及时将 exchange 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 事件详情

CVE-2021-26855: 服务端请求伪造漏洞

Exchange 服务器端请求伪造（SSRF）漏洞，利用此漏洞的攻击者能够发送任意 HTTP 请求并通过 Exchange Server 进行身份验证。

CVE-2021-26857: 序列化漏洞

Exchange 反序列化漏洞，该漏洞需要管理员权限，利用此漏洞的攻击者可以在 Exchange 服务器上以 SYSTEM 身份运行代码。

CVE-2021-26858/CVE-2021-27065: 任意文件写入漏洞

Exchange 中身份验证后的任意文件写入漏洞。攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。该漏洞可以配合 CVE-2021-26855 SSRF 漏洞进行组合攻击。

五、 影响版本

产品名称	影响版本
exchange	2010/2013/2016/2019

六、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-26855	服务端请求伪造	泄漏服务器真实地址/权限中继/突破限制访问内部网络	严重
CVE-2021-26857	序列化	任意代码执行	严重
CVE-2021-26858	文件上传	上传恶意文件	严重
CVE-2021-27065	文件上传	上传恶意文件	严重

七、 安全建议

(一) 通用修补方案

微软已发布相关安全更新，用户可跟进以下链接进行升级:

CVE-2021-26855: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

CVE-2021-26857: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

CVE-2021-26858: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858

CVE-2021-27065: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

(二) 临时修补方案

CVE-2021-26855:

可以通过以下 Exchange HttpProxy 日志进行检测:

%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy

通过以下 Powershell 可直接进行日志检测:

Import-Csv -Path (Get-ChildItem -Recurse -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -

Filter ‘*.log’).FullName | Where-Object { $_.AuthenticatedUser -eq ” -and $_.AnchorMailbox -like ‘ServerInfo~*/*’ } | select DateTime, AnchorMailbox

如果检测到了入侵，可以通过以下目录获取攻击者采取了哪些活动

%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging

CVE-2021-26858:

日志目录：C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog

可通过以下命令进行快速浏览:

findstr /snip /c:”Download failed and temporary file” “%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog*.log”

写入的文件位于： %PROGRAMFILES%\Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp 目录，注意检测该目录有没有 webshell 等恶意程序

CVE-2021-26857:

该漏洞利用难度稍高，可利用以下命令检测日志条目

Get-EventLog -LogName Application -Source “MSExchange Unified Messaging” -EntryType Error | Where-Object { $_.Message -like “*System.InvalidCastException*” }

CVE-2021-27065:

通过以下 powershell 命令进行日志检测，并检查是否遭到攻击:

Select-String -Path “$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\ECP\Server*.log” -Pattern ‘Set-.+VirtualDirectory’

八、 参考链接

1. HAFNIUM targeting Exchange Servers with 0-day exploits

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危