安全漏洞通告

Cisco Jabber 多个高危漏洞风险通告

360CERT
北京奇虎科技有限公司 | 2021-03-25

报告信息

报告名称	Cisco Jabber 多个高危漏洞风险通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-032501
报告版本	1	**报告日期**	2021-03-25
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	2021-03-25	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	拒绝服务
CVE 编号	CVE-2021-1418 等
相关厂商	cisco
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.9
修复方案	通用修补方案
漏洞发布时间	2021-03-25
报告生成时间	2021-03-25

二、 漏洞简述

2021 年 03 月 25 日，360CERT 监测发现 Cisco 发布了 Jabber 的安全更新风险通告，漏洞编号为 CVE-2021-1411,CVE-2021-1469,CVE-2021-1417,CVE-2021-1471,CVE-2021-1418 ，漏洞等级：严重，漏洞评分：9.9。该漏洞目前尚未被广泛利用。

Cisco Jabber 是一个网络会议和即时消息传递应用程序，允许用户通过可扩展消息传递和状态协议（XMPP）发送消息。

对此，360CERT 建议广大用户及时将 Cisco Jabber 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、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.9

四、 漏洞详情

CVE-2021-1411: 代码执行

CVE: CVE-2021-1411

组件: jabber

漏洞类型: 代码执行

影响: 服务器接管

简述: 此漏洞是由于邮件内容验证不正确引起的。攻击者可以通过向受影响的软件发送特制的 XMPP 消息来利用此漏洞。成功的利用可使攻击者在目标系统上执行任意程序。

CVE-2021-1469: 代码执行

CVE: CVE-2021-1469

组件: jabber

漏洞类型: 代码执行

影响: 服务器接管

简述: 此漏洞是由于邮件内容验证不正确引起的。攻击者可以通过向受影响的软件发送特制的 XMPP 消息来利用此漏洞。成功的利用可使攻击者在目标系统上执行任意程序。

CVE-2021-1417: 信息泄露

CVE: CVE-2021-1417

组件: jabber

漏洞类型: 信息泄露

影响: 身份信息泄漏

简述: 攻击者可以通过将精心制作的 XMPP 消息发送到目标系统来利用此漏洞。成功利用此漏洞可使攻击者获取敏感的身份验证信息。

CVE-2021-1471: 证书校验

CVE: CVE-2021-1471

组件: jabber

漏洞类型: 证书校验

影响: 通信、流量劫持

简述: 攻击者可以通过在网关处拦截受影响软件的网络请求并提供恶意制作的证书，从而利用此漏洞。成功的利用可能使攻击者能够检查或修改 Cisco Jabber 客户端与服务器之间的请求内容。

CVE-2021-1418: 拒绝服务

CVE: CVE-2021-1418

组件: jabber

漏洞类型: 拒绝服务

影响: 应用程序宕机

简述：攻击者可以通过将精心制作的 XMPP 消息发送到目标系统来利用此漏洞。成功的利用可使攻击者执行 DDos 攻击，导致应用程序宕机。

五、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-1418	拒绝服务	应用程序宕机	中危
CVE-2021-1471	证书校验	通信、流量劫持	中危
CVE-2021-1417	信息泄露	敏感数据泄漏	中危
CVE-2021-1469	代码执行	服务器接管	严重
CVE-2021-1411	代码执行	服务器接管	严重

六、 安全建议

(一) 通用修补方案

Cisco Jabber 是一个商业软件，思科已经发布了免费软件更新，以解决此通报中描述的漏洞。购买了软件的客户可以直接通过更新应用完成漏洞修复。

可通过以下 Cisco 官网链接下载 Jabber 最新版：

https://www.webex.com/downloads/jabber.html

七、 产品侧解决方案

(一) 360AISA 全流量威胁分析系统

针对微软本次安全更新，360AISA 已基于流量侧提供对应检测能力更新，请 AISA 用户联系 techsupport@360.cn 获取更新，尽快升级检测引擎和规则，做好安全防护工作。

(二) 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

八、 参考链接

1. Cisco Jabber Desktop and Mobile Client Software Vulnerabilities

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-jabber-PWrTATTC

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