安全漏洞通告

ntopng 权限绕过与任意代码执行漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-03-24

报告信息

报告名称	ntopng 权限绕过与任意代码执行漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-032401
报告版本	1	**报告日期**	2021-03-24
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	2021-03-24	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	权限绕过/代码执行
CVE 编号	CVE-2021-28073 等
相关厂商	ntop
相关组件	ntopng
威胁等级	高危
影响面	一般
360CERT 评分	8.0
修复方案	临时修补方案
漏洞发布时间	2021-03-24
报告生成时间	2021-03-24

二、 漏洞简述

2021 年 03 月 23 日，360NoahLab 发布了关于 ntopng 的风险通告，漏洞编号为 CVE-2021-28073/CVE-2021-28074 ，漏洞等级： 高危 ，漏洞评分：8.0 。

ntopng 是一套开源的网络流量监控工具，提供基于 Web 界面的实时网络流量监控。支持跨平台，包括 Windows、Linux 以及 MacOS。ntopng 使用 C++ 语言开发，其绝大部分 Web 逻辑使用 lua 开发。

同时 ntopng 被部分路由器或者网络设备作为底层组件用于监控和梳理所在环境的网络流程情况。建议用户结合自身情况进行检查和修复。

ntopng 官方已于 2021 年 03 月 05 日发布修复代码于 github 仓库

对此，360CERT 建议广大用户及时将 ntopng 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	高危
影响面	一般
360CERT 评分	8.0

四、 漏洞详情

涉及漏洞 CVE 如下：

- CVE-2021-28073

- CVE-2021-28074

漏洞利用的核心在于对于 ntopng web 接口的权限认证绕过，导致攻击者可以在未授权的情况下请求复合漏洞利用条件的接口，并最终利用 ssrf 漏洞和高危服务实现代码执行。

五、 安全建议

(一) 临时修补方案

ntopng 已经在 github 的 commit e8b9721479f401f595c5c7bb151819aceb03ad71 中修复了核心的权限绕过漏洞，但由于自行编译并应用到指定设备的实施难度较大。

360CERT 建议：排查使用 ntopng 的服务，并将 ntopng 的相关端口禁止从互联网访问

六、 参考链接

1. ntopng 流量分析工具多个漏洞分析

   http://noahblog.360.cn/ntopng-multiple-vulnerabilities/

2. Fixes string truncation possibly causing limited auth bypass

   https://github.com/ntop/ntopng/commit/e8b9721479f401f595c5c7bb151819aceb03ad71

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