Ntopng 权限绕过/服务端请求伪造漏洞通告

2021 年 4 月 23 日

目录

一、 漏洞概要

漏洞名称	Ntopng 权限绕过漏洞 CVE-2021-28073/Ntopng 服务端请求伪造漏洞 CVE-2021-28074
影响组件	ntopng
影响范围	ntopng<4.2
漏洞类型	权限绕过 服务端请求伪造
利用条件	1、用户认证：不需要用户认证 2、触发方式：远程
综合评价	CVE-2021-28073 <综合评定利用难度>：容易，无需授权即可远程代码执行。 <综合评定威胁等级>：高危，能修改管理员密码。 CVE-2021-28074 <综合评定利用难度>：一般，需要在局域网内模拟 SSDP 应答。 <综合评定威胁等级>：高危，能伪造 session，特定版本可以造成命令执行。

二、 漏洞分析

2.1 组件介绍

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。

2.2 漏洞描述

2021 年 3 月 24 日，深信服安全团队监测到一则 ntopng 组件存在权限绕过和服务端请求伪造漏洞的信息，漏洞编号：CVE-2021-28073、CVE2021-28074，漏洞危害：高危。

Ntopng 权限绕过漏洞 CVE-2021-28073

由于 ntopng 声明了一个大小为 255 的字符串数组来储存用户请求的文件路径导致了该漏洞的产生。并针对以非.lua 扩展名结尾的路径后补充了.lua，攻击者可利用该漏洞在未经授权的情况下，构造恶意数据绕过 URL 访问控制结合特定版本可造成密码重置、文件包含。

Ntopng 服务器请求伪造漏洞 CVE-2021-28074

该漏洞是由于 ntopng 在收到 SSDP 响应是没做任何校验，攻击者可利用该漏洞在未经授权的情况下，构造恶意的 SSDP 响应数据造成 SSRF，结合特定版本可造成 session 伪造、命令执行。

2.3 漏洞复现

搭建 ntopng 组件 3.2 版本环境，复现漏洞 CVE-2021-28073，

效果如下：


Raw
Params
Headers
Hex
GET
/lua
/../..
word_reset
.lua.38 HTTP/1.1
Host:
:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: user=admin
Upgrade-Insecure-Requests: 1
Raw
Headers
Hex
HTTP/1.1 200 OK
Cache-Control: max-age=0, no-cache, no-store
Server: ntopng 3.2.171227 [Debian buster/sid [x86_64]]
Pragma: no-cache
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: session=; max-age=3600; path=/; HttpOnly
Content-Type: text/html; charset=utf-8
Last-Modified: Thu, 01 March 2021 08:18:41 GMT
{ 'result' : -1, 'message' : 'Invalid parameters' }

三、 影响范围

ntopng 是在 GPLv3 下发布的基于 Web 的网络流量监视应用程序。全球互联网中有上万台服务器运行该服务，可能受漏洞影响的资产广泛分布于世界各地，中国大陆省份中主要分布于北京、广东、浙江等地。

目前受影响的 Ntopng 版本：Ntopng<4.2

四、 解决方案

4.1、 官方解决方案

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。

链接如下：https://github.com/ntop/ntopng

4.2、 如何检测组件系统版本

登录 web 界面首页即可查看：