**漏洞报告**

漏洞编号: CVE-2021-44790

漏洞描述:

精心设计的请求主体可能会导致 mod\_lua 多部分解析器（从 Lua 脚本调用 r:parsebody()）中的缓冲区溢出。 Apache httpd 团队并不清楚该漏洞的利用，尽管这是有可能被制作的。此漏洞会影响 Apache HTTP Server 2.4.51 及更早版本。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2021-44790>

漏洞披露时间: 12/20/2021

漏洞参考链接: 见下面的各个链接

野外漏洞报告：

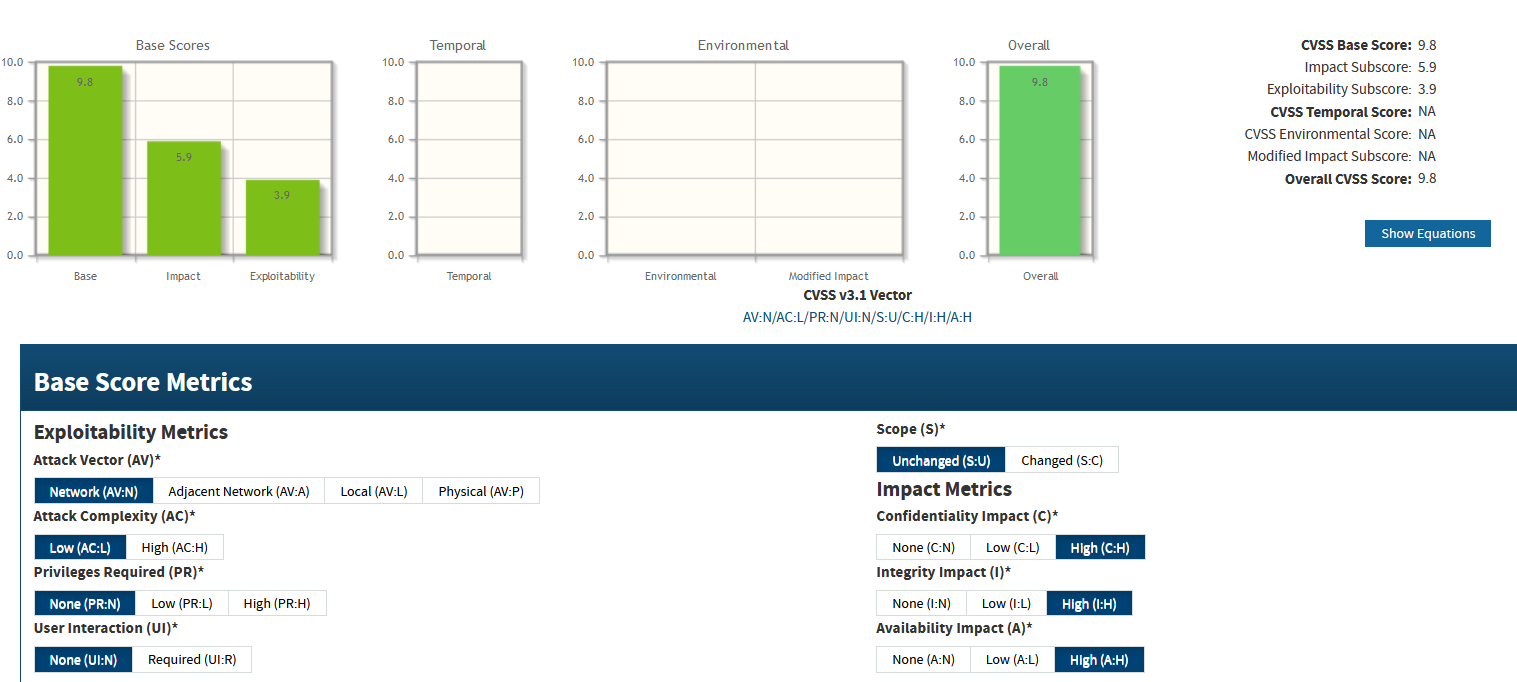
链接:

<https://www.zerodayinitiative.com/blog/2022/1/25/cve-2021-44790-code-execution-on-apache-via-an-integer-underflow>

漏洞类型: 网络远程攻击漏洞

漏洞危害: 未经身份验证的远程攻击者可以通过向目标服务器发送精心设计的请求来利用此漏洞。成功利用可能导致在服务器进程的安全上下文下远程执行代码，而不成功的攻击可能导致拒绝服务条件。

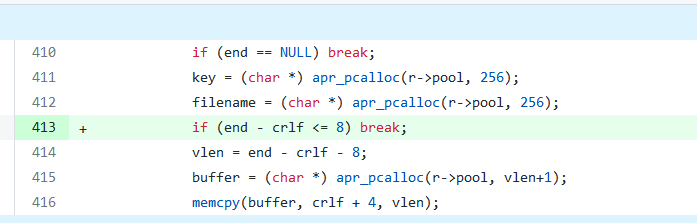
CVSS评分: 9.8(已检验)



漏洞影响的组件版本:

Apache http\_server: 2.4.52之前的版本

在2.4.52版本之前都没有添加对于字符串长度的检验，会导致缓存区溢出攻击，在2.4.52版本加入了以下的判断，这样避免了长度溢出：



Fedoraproject fedora 34 - 36版本

Debian debian\_linux 10.0 , 11.0

Tenable tenable.sc 5.16.0 - 5.20.0

Netapp cloud\_backup

Oracle communications\_operations\_monitor 4.3 , 4.4 , 5.0

Oracle communications\_element\_manager 9.0之前的版本

Oracle communications\_session\_report\_manager 9.0之前的版本

Oracle communications\_session\_route\_manager 9.0之前的版本

Oracle http\_server 12.2.1.3.0 , 12.2.1.4.0

Oracle instantis\_enterprisetrack 17.1 - 17.3

Oracle zfs\_storage\_appliance\_kit 8.8

Apple mac\_os\_x 10.15.7 security\_update\_2020-001

Apple mac\_os\_x 10.15.7 security\_update\_2021-001 - 2021-008

Apple mac\_os\_x 10.15.7 security\_update\_2022-001 - 2022-003

Apple macos 10.15.7之前的版本

Apple macos 11.0 - 11.6.6

Apple macos 12.0 - 12.4

漏洞修复的组件版本: Apache http\_server: 2.4.52

漏洞成因:

精心设计的请求主体可能会导致 mod\_lua 多部分解析器中的缓冲区溢出，这可能会导致代码在安全进程的上下文中执行。Apache httpd 的 mod\_lua 模块中出现了一个整数溢出漏洞。该漏洞是由于模块的多部分解析器中的请求主体验证不正确，通过 Lua 脚本中的 r:parsebody() 函数调用。未经身份验证的远程攻击者可以通过向目标服务器发送精心设计的请求来利用此漏洞。成功利用可能导致在服务器进程的安全上下文下远程执行代码，而不成功的攻击可能导致拒绝服务条件。

漏洞位置:

参考链接: <https://www.venustech.com.cn/new_type/aqldfx/20220120/23400.html>

根据漏洞公告，可知漏洞存在于mod\_lua模块中，lua脚本调用了r:parsebody()函数发生了缓冲区溢出。结合patch信息，直接定位到req\_parsebody函数内。

漏洞PoC：

链接: <https://github.com/GloryToMoon/POC_codes/blob/main/CVE-2021-44790-checker.py>

漏洞补丁：

链接:

<https://github.com/apache/httpd/commit/07b9768cef6a224d256358c404c6ed5622d8acce>

备注: 该漏洞在Apache HTTP Server 2.4.52中进行了修复。在内存申请之前，增加了对长度的合法性校验。

漏洞处置建议：

链接: <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFSWOH4X77CV7AH7C4RMHUBDWKQDL4YH/>

将Apache http\_server组件更新到2.4.52版本以上