山西省互联网网络安全预警信息通报

山西省通信管理局
主办：国家计算机网络应急技术处理协调中心山西分中心　2021 年 4 月 23 日

关于 Google V8 引擎远程代码执行漏洞导致微信等软件存在关联漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了微信 Windows 客户端远程代码执行漏洞（CNVD-2021-29068）。攻击者利用该漏洞，通过发送钓鱼链接并引诱用户点击，可获取远程主机控制权限。目前，漏洞细节尚未公开，厂商已发布新版本完成修复。此漏洞是 Google V8 引擎历史漏洞的衍生关联漏洞。

一、漏洞情况分析

美国谷歌（Google）公司开发维护的 V8 引擎是一款开源 JavaScript 引擎，通过将 JavaScript 代码编译成原生机器码，并使用内联缓存等多种技术提高脚本的编译和执行性能。V8 引擎支持多操作系统，具有较好的可移植和跨平台特

性。V8 引擎支持多种宿主环境的嵌入，实现 JavaScript 语言在多个领域中的应用。

V8 引擎不仅被广泛应用于 Google Chrome、Microsoft Edge 等网页浏览器软件中，而且在内置网页浏览功能的软硬件（服务）产品中得到了广泛应用，异步服务器框架 Node.js 也使用 V8 引擎解析 JavaScript。V8 引擎存在的安全缺陷会对内嵌 V8 引擎的软硬件产品和服务造成影响，导致关联漏洞的发生。

近几年，V8 引擎曾多次被研究者发现存在高危漏洞。其中，Google V8 引擎远程代码执行漏洞（CNVD-2021-29059，对应 CVE-2021-21220）相关细节已公开，谷歌公司尚未发布新版本修复该漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意页面，诱导受害者访问，实现对浏览器的远程代码执行或者拒绝服务攻击,但攻击者单独利用上述漏洞无法实现沙盒（SandBox）逃逸。沙盒是 Google Chrome 浏览器的安全边界，防止恶意攻击代码破坏用户系统或者浏览器其他页面。沙盒保护模式在 Google Chrome 浏览器中默认开启。CNVD 对该漏洞的综合评级为“高危”。

2021 年 4 月 17 日，国家信息安全漏洞共享平台收录了微信 Windows 客户端远程代码执行漏洞，此漏洞是 Google V8 引擎历史漏洞的衍生关联漏洞。微信客户端（Windows 版本）使用 V8 引擎解析 JavaScript 代码，并关闭了沙盒模式

（--no-sandbox 参数）。攻击者利用上述漏洞，构造恶意钓鱼链接并通过微信发送，在引诱受害者使用微信客户端（Windows 版）点击钓鱼链接后，可获取远程主机的控制权限，实现远程代码执行攻击。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

Google V8 引擎漏洞导致的关联漏洞产品包括:

GoogleChrome < = 90.0.4430.72

MicrosoftEdge 正式版（ 89.0.774.76）

微信 Window 版客户端 < 3.2.1.141

内嵌 V8 引擎的软硬件产品和服务

三、处置措施

目前，谷歌、微软公司尚未发布新版本修复关联漏洞，CNVD 建议用户使用 Chrome、Edge 等浏览器时不要关闭默认的沙盒模式，谨慎访问来源不明的文件或网页链接，并及时关注厂商的更新公告。

腾讯公司已发布微信新版本修复该漏洞，建议用户立即将微信 （Windows 版）更新至最新版本。

产品内嵌谷歌 V8 引擎的软硬件（服务）厂商应对集成的 V8 引擎版本进行自查，更新引擎至最新版本，同时及时关注谷歌公司的安全更新公告，并通过沙盒模式调用该引擎。

附: 参考链接:

https://twitter.com/frust93717815/status/1382301769577861123

https://www.google.com/chrome/

https://mp.weixin.qq.com/s/qAnxwM1Udu1j1K3Wn2awVQ

https://paper.seebug.org/1557/