Firefox 远程代码执行漏洞（CVE-2019-11707）预警通告

文档信息

编号	QiAnXinTI-SV-2019-0013
关键字	Firefox RCE CVE-2019-11707
发布日期	2019 年 06 月 19 日
更新日期	2019 年 06 月 19 日
TLP	WHITE
分析团队	奇安信威胁情报中心红雨滴安全研究团队

通告背景

近日，火狐浏览器官方发布安全更新，修复了一个存在于 Firefox 全平台所有版本中的远程代码执行漏洞，火狐开发人员称此漏洞已经被用于野外攻击。

Mozilla Foundation Security Advisory 2019-18

Security vulnerabilities fixed in Firefox 67.0.3 and Firefox ESR 60.7.1

Announced June 18, 2019

Impact critical

Products Firefox, Firefox ESR

Fixed in Firefox 67.0.3
Firefox ESR 60.7.1

 # CVE-2019-11707: Type confusion in Array.pop

Reporter Samuel Groß of Google Project Zero, Coinbase Security

Impact critical

Description
A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw.

References
Bug 1544386

该火狐以及其企业版浏览器 0day 漏洞是由谷歌 Project Zero 团队的研究员 Samuel Groß和 Coinbase 安全团队发现，攻击者可能利用此漏洞通过诱使用户访问恶意网页触发漏洞从而获得对用户系统的控制。

漏洞概要

漏洞名称	Firefox 远程代码执行漏洞				
威胁类型	远程代码执行	**威胁等级**	严重	**漏洞 ID**	CVE-2019-11707
利用场景	攻击者可能会通过欺骗未修补的 Firefox 版本的用户访问恶意制作的网页，触发类型混淆漏洞获取任意代码执行从而控制用户系统。				
受影响系统及应用版本					
低于 Firefox 67.0.3 的所有平台所有版本 低于 Firefox ESR 60.7.1 的所有平台所有版本					

漏洞描述

该漏洞是由于 Array.pop 中的问题导致操纵 JavaScript 对象时可能会出现类型混淆，导致崩溃可利用。目前在野外存在使用这个漏洞进行定向攻击的案例。

攻击者可能会通过欺骗未修补的 Firefox 版本的用户访问恶意制作的网页或者网站，随后在他们的系统上执行任意代码来触发类型混淆，从而导致任意代码执行并控制目标设备。

影响面评估

由于该远程代码执行漏洞存在与火狐除最新外的所有版本中，因此浏览器若没有开启自动更新或者在内网运行的情况下，影响巨大。

目前该漏洞没有公开的利用代码，但据可靠消息已经被用于真实的定向攻击，漏洞利用代码扩散并被用于大规模攻击的可能性极高，请务必重视。

处置建议

Firefox 67.0.3 和 Firefox ESR 60.7.1 中修复了安全漏洞，请按以下链接更新

适用于 Windows 64 位的 Firefox 67.0.3
https://download.mozilla.org/?product=firefox-latest-ssl&os=win64&lang=en-US

Firefox 67.0.3 for Windows 32 位
https://download.mozilla.org/?product=firefox-latest-ssl&os=win&lang=en-US

适用于 macOS 的 Firefox 67.0.3
https://download.mozilla.org/?product=firefox-latest-ssl&os=osx&lang=en-US

Firefox 67.0.3 for Linux 64 位
https://download.mozilla.org/?product=firefox-latest-ssl&os=linux64&lang=en-US

Firefox 67.0.3 for Linux 32 位
https://download.mozilla.org/?product=firefox-latest-ssl&os=linux&lang=en-US

参考资料

https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/#CVE-2019-11707