Chrome v8 越界读写
漏洞通告

2021 年 9 月 28 日

目录

一、 漏洞概要

漏洞名称	Chrome v8 洞 越界读写漏洞 CVE-2021-30632
影响组件	Chrome v8
影响范围	Chrome < 93.0.4577.82
漏洞类型	越界读写
利用条件	1、用户认证：不需要用户认证 2、前置条件：需用户访问恶意网页 3、触发方式：远程
综合评价	<综合评定利用难度>：一般，用户访问恶意网页可以造成远程代码执行。 <综合评定威胁等级>：高危，能造成远程代码执行。

二、 漏洞分析

2.1 组件介绍

Google Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具。Google Chrome 的特点是简洁、快速。Google Chrome 支持多标签浏览，默认情况下，每个标签页面都在独立的“沙箱”内运行，在提高安全性的同时，一个标签页面的崩溃也不会导致其他标签页面被关闭。此外，Google Chrome 基于更强大的 JavaScript V8 引擎，提升浏览器的处理速度。

2.2 漏洞描述

2021 年 9 月 23 日，深信服安全团队监测到一则 Chrome 组件存在越界读写漏洞的信息，漏洞编号：CVE-2021-30632，漏洞威胁等级：高危。

Chrome V8 中存在越界读写漏洞，攻击者可利用该漏洞在未授权的情况下，构造恶意数据造成远程代码执行攻击，最终获取服务器最高权限。

三、 影响范围

Chrome 可以运行在几乎所有计算机平台上，由于其跨平台和安全性被广泛使用，成为最流行的浏览器软件。Chrome 在中国浏览器市场占有率最高，拥有广泛的用户基础。。

目前受影响的 Chrome 版本：

Chrome < 93.0.4577.82VMware vCenter Server 6.7

四、 解决方案

4.1、官方解决方案

当前官方已发布受影响版本的安全更新，建议受影响的用户及时更新。链接如下：

https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html

4.2、如何检测组件系统版本

在 Chrome 中选择设置，在设置界面点击关于 Chrome 即可看到当前版本。