网络安全预警通报

2023 年第 5 期 （总第 42 期）

西安交通大学网络信息中心 2023 年 11 月 20 日

【预警类型】 **高危预警**

【预警内容】

关于国内众多主流软件存在任意文件读取的漏洞

一、漏洞概述

微信、支付宝、小米浏览器、携程应用等国内主流软件均存在任意文件读取漏洞。此漏洞源于谷歌浏览器内核漏洞，而国内很多 app，包括苹果内置浏览器均为谷歌浏览器，故影响全系列产品。

二、漏洞详情

Google Chrome 是一款由 Google（谷歌）公司开发的网页浏览器。该浏览器基于开源内核（如 WebKit）编写，目标是提升稳定性、速度和安全性，并创造出简单且有效率的使用者界面。

WebKit 默认使用的 xsl 库(Libxslt),调用 document()加载的文档里面包含对外部实体的引用。

攻击者可以创建并托管包含 XSL 样式表的 SVG 图像和包含外部实体引用的文档。

当受害者访问 SVG 图像链接时,浏览器会解析 XSL 样式表,调用 document() 加载包含外部实体引用的文档，读取受害者机器的任意文件。

漏洞影响范围：

受影响的类型	受影响版本号
Chrome	116.0.5845.96
Chromium	116.0.5845.96
Electron	26.1.0

三、处置建议

1、升级应用内置浏览器版本；

2、用户不要点击陌生链接，防止被攻击

参考链接：

https://mp.weixin.qq.com/s/8XbqaAf6JYl39VREVHfuDA