保安资讯 - 今日重点 (2018/05/07)

微软修复原始数据区全面复制漏洞

CVE-2018-8344 | CVSS 3.0: 7.8 | 本地权限提升 | 已有公开 PoC | 微软 Windows 全版本受影响

微软修复 Windows 内核原始数据区（Raw Data Area）全面复制漏洞 CVE-2018-8344，该漏洞允许本地攻击者通过特殊 IOCTL 调用绕过内核内存保护机制，将任意内核数据复制到用户模式缓冲区，可用于泄露内核地址布局以辅助后续提权。微软于 2018 年 5 月 8 日发布修复，涵盖 Windows 7 SP1 至 Windows 10 1803 全版本。

CVE-2018-8344 | CVSS 3.0: 7.8 | Local Privilege Escalation | Public PoC | Affects Windows 7 SP1 – Windows 10 1803

- CVE-2018-8344 | CVSS 3.0: 7.8 | Raw Data Area 全面复制漏洞 | 微软 Windows 全版本
- 漏洞类型：内核内存泄露 → 辅助后续提权
- 受影响：Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows 8.1 / Windows 10 1803
- 修复版本：KB4284826 (Windows 10 1803) / KB4284819 (Windows 7 SP1)
- 公开 PoC：GitHub 上已有多个实现，可稳定泄露内核地址
- 建议：立即安装 KB4284826 / KB4284819，优先级 P1

在线版本更严格导入策略导致 PDF/JS 绕过

CVE-2018-5158 | CVSS 3.0: 6.5 | 信息泄露 | 已有公开 PoC | 影响 Firefox 59.0.2 及早期版本

Firefox 59.0.2 修复 PDF.js 在线版本导入策略过宽导致 JS 绕过问题 CVE-2018-5158，攻击者可通过特殊 PDF 文件绕过 PDF.js 的 JS 执行限制，在受害者浏览器中执行任意脚本，可用于窃取 Cookie 或发起 CSRF 攻击。

CVE-2018-5158 | CVSS 3.0: 6.5 | Information Disclosure | Public PoC | Affects Firefox 59.0.2 and earlier

- CVE-2018-5158 | CVSS 3.0: 6.5 | PDF.js 在线版本导入策略过宽 | Firefox 59.0.2 及早期版本
- 漏洞类型：信息泄露 → 绕过 PDF.js 限制执行 JS 脚本
- 受影响：Firefox 59.0.2 及早期版本
- 修复版本：Firefox 59.0.3 / Firefox 60.0
- 公开 PoC：已有多个实现，可稳定绕过 PDF.js 限制
- 建议：立即升级 Firefox 59.0.3 / 60.0