

互联网疫情 警示

07/07/2009

赛门铁克中国安全响应中心

内容

[总述](#)

[技术分析](#)

[补丁](#)

[应对和防范](#)

[反病毒更新](#)

[IPS 更新](#)

互联网疫情警示

----微软视频控件漏洞风险及应对

07/07/2009

总述

2009年7月，微软操作系统被曝出新的视频控件漏洞（Vulnerability in Microsoft Video Streaming ActiveX control）。到目前为止，微软尚未发布针对此漏洞的官方补丁或系统更新。而针对该漏洞的恶意攻击已经开始行动，中国和亚洲其他地区受影响较大。因此，计算机用户面临极大的潜在威胁。赛门铁克将继续密切监测和研究针对该视频控件漏洞的病毒，并将为用户提供及时的通报和应对措施。

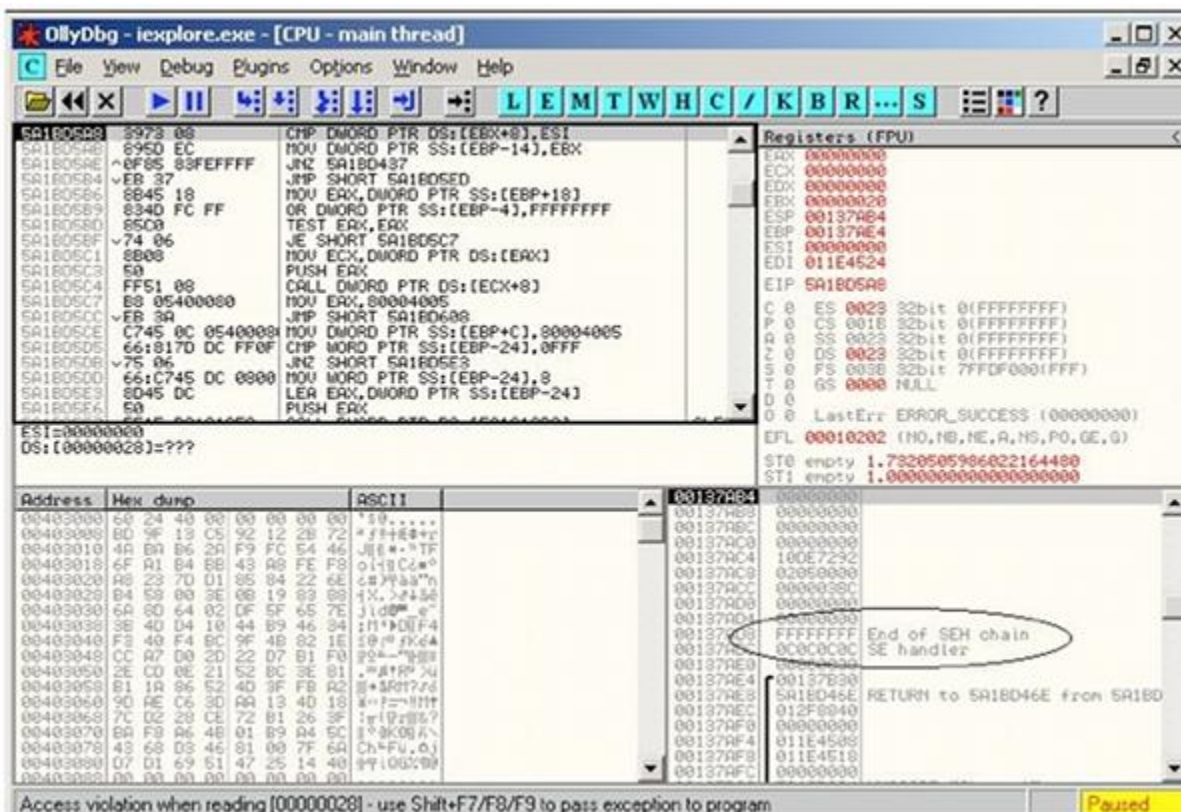
目前，Windows XP 及 Windows Server 2003 受该漏洞影响最大，而 Windows Vista 和 Windows Server 2008 暂时不受影响。

技术分析

该视频控件漏洞位于系统文件 msvidctl.dll。目前针对该漏洞的攻击主要通过特殊构造的 Javascript 调用伪装为.gif 后缀的病毒文件，将其作为 ActiveX 对象“BDATuner.MPEG2TuneRequest.1”的“data”参数传入。该 ActiveX 对象的 CLSID 为 0955AC62-BF2E-4CBA-A2B9-A63F772D46CF。

当系统文件 msvidctl.dll 解析该.gif 文件时，会出现溢出并覆写结构化异常处理函数，将函数指针变为 0x0C0C0C0C。而 0x0C0C0C0C 这个地址恰好位于堆区，攻击者可以利用堆扩散技术载入恶意代码。因此，当用户访问某些含有这类特别构造的文件的恶意网站时，漏洞便会被触发，攻击者可获取与当前计算机用户同等的操作权限，下载恶意文件至计算机中，并在受感染计算机中远程执行恶意代码。

```
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030h: 00 00 00 00 00 00 FF FF FF FF 0C 0C 0C 0C 00
```



补丁

目前为止，还没有任何官方补丁可以完全修补此漏洞。

应对和防范

赛门铁克建议用户采取以下措施：

- 禁止该 ActiveX 控件在 Internet Explorer 中运行
- 禁止 Internet Explorer 运行 JavaScript 脚本
- 避免访问不熟悉或可疑的网站
- 使用浏览器时尽量以普通用户身份登录。权限越大，可能受到的影响就越大
- 启动防火墙的入侵检测功能
- 及时更新安全软件的病毒定义

反病毒更新

赛门铁克已将针对该漏洞的攻击检测为 Downloader.Fostrem，由该病毒下载的恶意文件被检测为 Trojan Horse，Backdoor.Trojan，Infostealer 和 Downloader，并已发布相关的病毒定义。

IPS 更新

赛门铁克已发布的 IPS 入侵防御特征可主动监测可能针对此漏洞的攻击：

22920 - HTTP Malicious Toolkit Download Request

23086 - HTTP Malicious Toolkit Variant Activity