Risikoeinschätzung zur Schwachstelle in Internet Explorer (CVE-2013-3918)

14. November 2013

Klassifikation:
Öffentlich

IOprotect GmbH
Huobstrasse 14
8808 Pfäffikon SZ
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

Faktenlage

- Am 8. November informierte FireEye über gezielte Angriffe, die zwei bis anhin unbekannte Schwachstellen im Internet Explorer ausnutzen.
- Die eine Schwachstelle erlaubt es, die exakte Version einer bestimmten DLL auszulesen. Damit können Programm-Instruktionen aus den DLLs ausgelesen und für die Umgehung von DEP[1] genutzt werden. Diese Schwachstelle wird von Microsoft noch immer untersucht. Entsprechend ist keine CVE-Kennung dafür bekannt.
- Die zweite Schwachstelle (CVE-2013-3918) nutzt diese Informationen und ermöglicht das Ausführen von Befehlen auf einem verwundbaren System.
- Am 12. November 2013 publizierte Microsoft einen Patch (MS13-090) für die kritischere der beiden Schwachstellen (CVE-2013-3918). Details von Microsoft sind diesem Blogpost zu entnehmen.
- Die beiden Schwachstellen wurden in Kombination bereits seit mehr als einem Jahr in fortgeschrittenen Angriffen genutzt. In der Zwischenzeit wurden die Informationen darüber auch auf unterschiedlichen, öffentlichen Webseiten publiziert. Es dürfte damit nicht mehr lange dauern, bis Cyberkriminelle diese Schwachstelle aktiv und verbreitet ausnutzen.

[1] DEP = Data Execution Prevention

Risikoeinschätzung von IOprotect

IOprotect hat den kursierenden Exploit und die Schwachstelle analysiert. Diese lässt sich je nach System-Setup und Browser-Version unterschiedlich zuverlässig ausnutzen. Die Einschätzung von IOprotect, u.a. basierend auf dem untersuchten Exploit, sieht wie folgt aus:

Windows XP mit IE7 oder IE8

Die Schwachstelle lässt sich, basierend auf den vorhandenen Schutzmassnahmen auf OS-Ebene, einfacher ausnutzen als bei neueren Betriebssystemen. Es sind keine zusätzlichen Abhängigkeiten auf dem System notwendig (z.B. ASLR[2]-inkompatible DLLs). Das Risiko ist entsprechend hoch.

Windows Vista und Windows 7 mit IE7 oder IE8

Die Schwachstelle lässt sich ausnutzen, falls entweder eine alte Java-Installation (Java 6) oder Microsoft Office auf dem System installiert sind[3]. Das Risiko ist in dem Fall als hoch einzustufen.

Internet Explorer 9, 10

Die Schwachstelle ist auf beiden Browser-Versionen ebenfalls vorhanden und der Exploit führt auch zum Absturz der Browser. Allerdings wird der Code nicht ausgeführt. Das Risiko für den IE9 und IE10 wird für den untersuchten Exploit derzeit als gering eingeschätzt.

Risikoeinschätzung allgemein

Aufgrund der an die Öffentlichkeit gelangten Informationen zur Schwachstelle und dem Exploit ist das Risiko gestiegen. Firmen sollten den Patch im Advisory MS13-090 so rasch wie möglich einspielen und die Wirksamkeit der implementierten Gegenmassnahmen testen.

[2] ASLR = Address Space Layout Randomization

[3] Oder eine andere DLL, die nicht ASLR-kompatibel ist

Testen von Schutzmassnahmen

Da viele Firmen den Patch verspätet einspielen, ist die Wirksamkeit der vorhandenen Schutzmassnahmen (Next-Gen Firewalls, Web-Proxy, IDS/IPS, AV-Software etc.) entscheidend. Zu diesem Zweck hat IOprotect einen Test-Exploit für Windows XP, Vista und Windows 7 entwickelt, der zur Demonstration die Schwachstelle ausnutzt und den Windows-Rechner (calc.exe) auf dem System ausführt. Dieser Test-Exploit steht den Kunden von IOprotect seit dem 14. November 2013 zur Verfügung.