Risikoeinschätzung zur Schwachstelle in Internet Explorer (CVE-2013-3893)

26. September 2013

Klassifikation:
Öffentlich

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

Faktenlage

- Am 17. September 2013 publiziert Microsoft das Advisory 2887505, in dem sie vor gezielten Angriffen auf eine bis anhin unbekannte Schwachstelle in Internet Explorer warnen. Die Schwachstelle ist unter der Kennung CVE-2013-3893 bekannt. Betroffen sind der Internet Explorer 6, 7, 8, 9, 10 und 11.
- Am selben Tag publiziert Microsoft eine temporäre Lösung in Form eines Fix-It, der die Schwachstelle temporär schliesst.
- Die Schwachstelle wurde gemäss dem Internet Storm Center (ISC) bereits im August ausgenutzt, jedoch bei sehr gezielten Angriffen. Betroffen waren unter anderem Institutionen und Firmen in Japan. Das Internet Strom Center hat den Threat Level von grün auf gelb gesetzt.
- Detaillierte Informationen zum Exploit sind auf dem Blog von FireEye unter dem Titel „Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets“ zu finden.
- Der Exploit selber (das Angriffs-Script) ist auf öffentlich zugänglichen Webseiten publiziert worden. Es dürfte nicht lange dauern, bis Cyberkriminelle diese Schwachstelle aktiv und verbreitet ausnutzen werden.

Risikoeinschätzung von IOprotect

IOprotect hat den 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 IE6, IE7 oder IE8

Die Schwachstelle lässt sich, basierend auf den vorhandenen Schutzmassnahmen auf OS-Ebene, einfacher ausnutzen als bei Windows Vista/7/8. Es sind keine zusätzlichen Abhängigkeiten auf dem System notwendig (z.B. nicht ASLR-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 Update x) oder Microsoft Office auf dem System installiert sind[1]. Das Risiko ist in dem Fall als hoch einzustufen.

Internet Explorer 9

Die Schwachstelle lässt sich ausnutzen, falls eine Microsoft Office-Installation auf dem System vorhanden ist[2]. Das Risiko ist in dem Fall als hoch einzustufen.

Internet Explorer 10 und Internet Explorer 11

IE10 und IE11 verfügen über zusätzliche Schutzfunktionen (Virtual Table Guard, ForceASLR etc.). Die Schwachstelle ist dort zwar vorhanden, lässt sich aber ohne zusätzliche Schwachstelle nicht so einfach ausnutzen. Das Risiko mit dem IE10 und IE11 ist deshalb geringer einzustufen.

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

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

Risikoeinschätzung allgemein

Aufgrund der an die Öffentlichkeit gelangten Informationen zur Schwachstelle und dem Exploit ist das Risiko gestiegen. Firmen sollten den Fix-It von Microsoft einspielen und die Wirksamkeit der implementierten Gegenmassnahmen testen.

Testen von Schutzmassnahmen

Da viele Firmen den Fix-It nicht einspielen können oder wollen, 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 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 23. September 2013 zur Verfügung.