

Alert!**Patchday: Microsoft sichert XP und Vista ab, warnt vor neuem WannaCry**

14.06.2017 09:57 Uhr – Fabian A. Scherschel

vorlesen



In einem bisher nicht dagewesenen Schritt hat Microsoft am Patchday Updates für Windows-Versionen ausgeliefert, die nicht mehr unterstützt werden. Die Firma entschloss sich dazu, da sie weitere WannaCry-ähnliche Attacken befürchtet.

Wer noch Windows-XP- oder Vista-Rechner mit Internetanbindung betreibt, wird sich beim Anschalten heute Morgen gewundert haben: [Microsoft hat Updates für die beiden Betriebssysteme veröffentlicht](#), obwohl sie von der Firma eigentlich nicht mehr unterstützt werden. In einem bisher nie dagewesenen Schritt will [Microsoft damit weitere WannaCry-ähnliche Angriffe](#) verhindern. Der Verschlüsselungstrojaner hatte der Firma so stark zugesetzt, dass sie [Updates außer der Reihe veröffentlicht hatte](#) – auch für Vista und XP.

Microsoft befürchtet weitere Angriffe

Microsoft hat nach eigenen Angaben beim Stopfen der WannaCry-Lücken weitere Schwachstellen in Windows entdeckt, die für ähnliche Angriffe missbraucht werden könnten. Die Firma hält das offensichtlich für so wahrscheinlich, dass diese Lücken auch für Vista und XP mit Patches dicht gemacht wurden; obwohl dies eigentlich den eigenen Support-Grundsätzen widerspricht. Offiziell spricht Microsoft von einem "erhöhten Risiko" für Windows-Nutzer. Alle Windows-Versionen ab Windows XP und neuer werden über Microsofts Update-Dienste automatisch mit den Patches versorgt. Angesichts der ungewöhnlichen Entscheidung der Firma sollten Windows-Nutzer die Patches sofort installieren.

Genauere Details zu den Sicherheitslücken und der Art der befürchteten Angriffe hat Microsoft nicht mitgeteilt. Wer genau wissen will, welche Lücken Microsoft geschlossen hat, für den hat das Talos-Intelligence-Sicherheitsteam von Cisco [eine Liste mit CVE-Nummern zu den Patchpaketen von Microsoft](#) zusammengetragen. Die [offiziellen Release Notes](#) der Firma sind, wie neuerlich üblich, sehr spärlich und die [Patchliste](#) ist unübersichtlich.

Der Einsatz von XP ist nicht mehr verantwortbar

Obwohl Microsoft in diesem Fall Updates für XP und Vista verteilt hat, ist davon abzuraten, diese Betriebssysteme weiter einzusetzen. Sicherheitsforscher raten fast geschlossen von einem solchen Verhalten ab. Zu Zeiten von Schadcode-Wellen wie WannaCry haben stichprobenartige Tests von heise Security ergeben, dass XP-

Dienste

Security Consulter Emailcheck
 Netzwerkcheck Browsercheck
 Anti-Virus Krypto-Kampagne

heise devSec

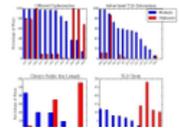
Im Oktober: Die Konferenz für sichere Software- und Webentwicklung

// heise
devSec()

Artikel

Cisco analysiert verschlüsselten Traffic, um Malware zu erkennen

Mit Hilfe von Machine Learning gelang es einer Forschergruppe, den verschlüsselten Netzwerk-Verkehr von Malware von regulärem zu unterscheiden – und das, ganz ohne ihn zu entschlüsseln.

**Windows-Diagnose: Programme und Prozesse meistern**

Wer mehr über das wissen will, was unter der Haube von Windows so vorgeht, kommt weder am Task-Manager noch am Sysinternals-Tool ProcMon vorbei.

**Analysiert: Alte Masche, neue Verpackung – Infektion durch PDFs**

Manipulierte Word-Dokumente sind bei Kriminellen beliebt, um Computer mit Malware zu infizieren. Dass auch PDF-Dateien ausführbaren Code enthalten können, ist hingegen ein wenig in Vergessenheit geraten. Eine unlängst grassierende Spam-Kampagne ist ein guter Grund, sich diese Gefahr anhand eines frischen Samples in Erinnerung zu rufen.



Rechner die mit dem Internet verbunden sind, zum Teil innerhalb von Minuten infiziert werden.

Gibt es also eine Lücke im Betriebssystem, für die Microsoft noch keine Patches verteilt hat, sind diese Rechner einem überdurchschnittlichen Risiko ausgesetzt. Anders sieht es nur aus, wenn Firmen viel Geld für außerordentlichen Support für diese Rechner an Microsoft zahlen. ([fab](#))

Kommentare lesen (416 Beiträge)

Forum zum Thema: **Desktopsicherheit**



<https://heise.de/-3743004>

Drucken

Mehr zum Thema [Sicherheitslücken](#) [WannaCry](#) [Windows Patchday](#) [Microsoft](#) [Windows XP](#) [Windows Vista](#)

Neueste Forenbeiträge

Na ist doch prima....

... dass Locky sich aktiver gegen Debugging wehrt. Der Trojaner soll etwa eine virtuelle Maschine erkennen und darin nicht laufen. Würden die...

Forum: [Erpressungstrojaner Locky ist zurück, be...](#)



von Cobolteufel; 23.06.2017 11:36

NEIN? Wer hätte denn jemals DAMIT gerechnet? voll gemein.

Demnächst missbrauchen solche Verbrecher noch unseren schönen Bundestrojaner. *Deutlich erhobener Zeigefinger* Böse, böse. Ihr fiesen...

Forum: [Windows-Trojaner nutzt NSA-Hintertür u...](#)



von Asgard-v-d-S; 23.06.2017 11:28

Danke für den Hinweis

Jetzt wissen die Malware Betreiber auch wie sie ihre "Signatur" fixen können ;)

Forum: [Cisco analysiert verschlüsselten Traffic, ...](#)



von hasufell; 23.06.2017 11:20

Der Kommentar



Warum Google uns echte Verschlüsselung verweigert



Warum haben wir eigentlich immer noch keine einfach zu nutzende Ende-zu-Ende-Verschlüsselung? Die Standardantwort lautet: Viel zu kompliziert! Doch das ist Unsinn; Apple zeigt längst, wie einfach das sein kann.

News und Artikel
News
7-Tage-News
News-Archiv
Hintergrund-Artikel

Service
Newsletter
Tools
Foren
RSS
mobil

Dienste
Security Consulter
Netzwerkcheck
Anti-Virus
Emailcheck
Browsercheck
Krypto-Kampagne