

[« vorige](#) | [nächste »](#)

Ähnliche Artikel

Alert! NSA-Hacking-Tools: Kritische Sicherheitslücke in FortiGate-Firewalls – jetzt patchen

18.08.2016 14:20 Uhr – Dennis Schirrmacher

vorlesen



Die Neuerungen von Linux 4.7

Die neue Kernel-Version unterstützt AMDs neue Grafikchips. Ferner soll Linux 4.7 das Stromsparpotenzial moderner Prozessoren stärker ausschöpfen und...

36

Build 2016 – eine Zusammenfassung zu Microsofts Entwicklerkonferenz

Einen Überblick für alle (.NET-)Entwickler, die sich eine kompakte Zusammenfassung zu den Neuigkeiten von Microsofts alljährlicher...

NSA zwischen James Bond und Big Brother

Die Aktivitäten der Equation-Gruppe und der gezielte Diebstahl von SIM-Karten-Schlüsseln zeigen sehr gut die zwei Gesichter der Geheimdienste.

6



(Bild: Screenshot)

Setzen Angreifer an einer Schwachstelle im FortiOS an, können sie Zugriff auf Systeme bekommen und die Kontrolle übernehmen.

FortiGate sichert sein Firewall-Betriebssystem FortiOS ab und stopft eine als kritisch eingestufte Sicherheitslücke. Davon sind alle Versionen bis einschließlich 4.x betroffen, [warnt der Anbieter](#) von Sicherheits-Lösungen.

Wer eine verwundbare Version einsetzt, sollte zügig auf den abgesicherten 5.x-Versionsstrang aktualisieren. Läuft auf einer Firewall die aktuelle Version von FortiOS nicht, stehen noch die gepatchten Versionen 4.1.11, 4.2.13 und 4.3.9 bereit.

Anfällig für NSA-Exploit?

Im Gegensatz zu [Cisco, die jüngst auch Sicherheits-Patches für eigene Firewalls](#) veröffentlicht haben, erwähnt FortiGate die geleakten NSA-Hacker-Waffen der Equation Group nicht als Auslöser für die Veröffentlichung des Sicherheits-Updates.

Ein Zusammenhang liegt in diesem Kontext aber nahe: Sicherheitsforscher sind [bei der Auswertung](#) des Leaks auch auf Exploits für FortiGate-Firewalls gestoßen. Eigenen Angaben zufolge prüft FortiGate aktuell weitere Produkte auf Verwundbarkeiten.

Um die Lücke auszunutzen, müsse ein Angreifer einfach authentifiziert sein, um aus der Ferne Admin-Rechte erlangen zu können. Ein Übergriff kann über eine manipulierte HTTP-Anfrage eingeleitet werden, beschreibt FortiGate.

Am vergangenen Wochenende hat die Hacker-Grupper Shadow Brokers von der Equation Group abgezogene [Hacker-Tools veröffentlicht](#). Mittlerweile [bestätigen mehrere Instanzen](#) die Echtheit der Exploits und legen nahe, dass die NSA hinter der Equation Group steckt; das wurde bisher nur vermutet. ([des](#))

[Kommentare lesen \(3 Beiträge\)](#)[« vorige](#) | [nächste »](#)Forum bei heise Security: [Serversicherheit](#)

Anzeige


Wir suchen zum nächstmöglichen Termin einen
Campaign Manager (m/w)
Für alle Informationen klicken Sie [hier](#).

Anzeige


Neue Browser mit Privatsphäre-Schutz
Lohnt sich die Cloud für Ihre Firma wirklich?
Enthüllen Sie Details mit 4K HDR
APIs: Wildwuchs vermeiden und Überblick behalten
Profitieren Sie von Big Data – einfach und schnell
Über 600 kostenlose eBooks für Bildung und Beruf
Hackathon "API/open" in Berlin
Mobile Geräte im Unternehmen sicher managen
Das Insider Portal – Fakten zu aktuellen IT-Themen

Weitere News zum Thema


Geleakte NSA-Exploits: Cisco patcht Zero-Day-Lücke

 Firewalls von Cisco sind verwundbar und Angreifer können unter Umständen eigenen Code ausführen und Systeme übernehmen. Sicherheits-Patches sind...
18. August 2016, 10:31 Uhr 58


Angebliche Hacker-Waffen der NSA zum Verkauf

 Eine Gruppe namens Shadow Brokers brüstet sich damit, Tools von der Hacker-Gruppe Equation Group abgezogen zu haben. Diese wird immer wieder in...
16. August 2016, 09:49 Uhr 46

Veröffentlichte NSA-Hackersoftware ist offenbar echt

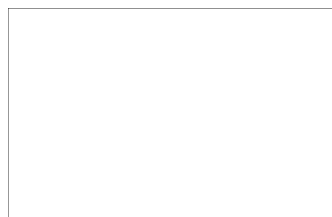
 US-Sicherheitsexperten und frühere NSA-Mitarbeiter befinden die Software, die Unbekannte am Wochenende veröffentlichten, als echt.
17. August 2016, 15:55 Uhr 138

Exploit-Kit Rig: Verbrechen lohnt sich wieder

 Vor einigen Monaten wurde der Quellcode des Exploit-Kits RIG 2.0 veröffentlicht; damit war der Shooting-Star der Crimeware-Szene erstmal aus dem...
06. August 2015, 11:40 Uhr 47

Themen im Trend

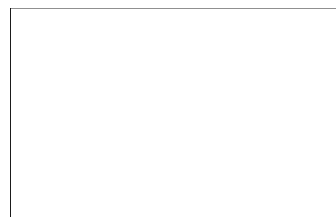
Fahrbericht: McLaren 540 C aus der neuen „Sports Series“



McLaren hat zwei Baureihen unterhalb des P1, also unterhalb der nun so genannten „Super Series“ bestehend aus diversen 650- und 675-Derivaten, die...

4

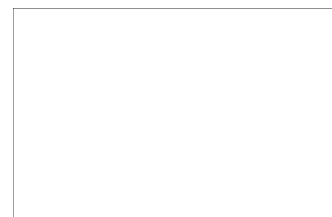
US-Einzelhandelsriese Target: Verkäufe von Apple-Geräten stark rückläufig



Das schlechte Geschäftsergebnis der Elektroniksparte ist auch auf gesunkene Verkäufe bei Apple-Geräten zurückzuführen, erklärte der...

18. August 2016, 16:11 Uhr

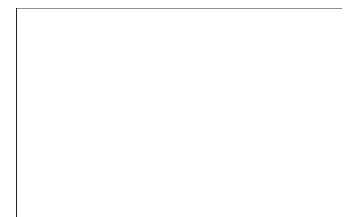
Jeep Willys MB: Der erste seiner Art



Als die Amerikaner einen ganzen Planeten befreien mussten, entstand der Willys MB – der UR-Jeep. Ein Auto, dessen Name heute ein Synonym für alle...

3

Bericht: "iPhone 7" heißt tatsächlich iPhone 7



Apple plant offenbar keine veränderte Namensgebung für seine nächste Smartphone-Generation. Zudem gibt es neue Spekulationen über Geräte mit 256...

18. August 2016, 10:34 Uhr

Elektroautos
Regierung will Ladesäulen für jedes Elektroauto öffnen



Elektroautos sollen in Deutschland künftig an jeder öffentlichen Ladesäule mit Strom versorgt werden können. Dazu will die...



EFF vs. Microsoft
Kritik an Upgrade-Praxis und Datensammelei von Windows 10



Microsoft wurde schon mehrfach heftig für seine Upgrade-Praxis für Windows kritisiert. Die Electronic Frontier Foundation hat die...

Gamescom
Civilization VI: Eigensinnige Despoten



Firaxis lässt im Herbst eine neue Inkarnation der traditionsreichen Strategieserie Civilization auf die Spielergemeinde los.



Star Trek Bridge Crew
Ende November auf Warp-Geschwindigkeit



Ubisoft will sein Weltraumspiel für alle drei VR-Systeme veröffentlichen. In Köln haben wir das kooperative Abenteuer für vier...



heise online
c't Magazin
iX Magazin
Technology Review
Mac & i
c't Fotografie

Telepolis
Make
heise Autos
heise Developer

heise Netze
Open Source
heise Security
heise Produkte

heise Video
TechStage
Download
Preisvergleich
Stellenmarkt

heise Events
IT-Markt
heise Business
Services
Tarifrechner
Shop

Artikel-Archiv
Abo
Loseblattwerke
RSS

Leserforum
Newsletter
Suche
iMonitor