Alert!

SambaCry: Erste Angriffe auf Linux-NAS-Boxen gesichtet

19.07.2017 18:46 Uhr – Fabian A. Scherschel vorlesen

(Bild: Loran Kloeze, heise online)

Die Hintertür in der SMB-Umsetzung von Linux-Systemen wird nun missbraucht, um gezielt NAS-Geräte anzugreifen. Für viele Geräte gibt es nur wenig Hoffnung, dass die Hersteller reagieren.

Die Sicherheitsfirma TrendMicro warnt davor, dass Angreifer momentan die SambaCry-Lücke in der SMB-Implementierung von Linux-Systemen (CVE-2017-7494) missbrauchen, um NAS-Geräte anzugreifen. Die ersten Angriffe auf Linux-Rechner mittels dieser Hintertür wurden vor ungefähr einem Monat bekannt, als Forscher einen Trojaner entdeckten, der Linux-Server angreift, übernimmt und sie dann zum Schürfen der Kryptowährung Monero missbraucht. Jetzt nutzen die Angreifer offenbar diesen Infektionsweg, um gezielt NAS-Geräte zu kompromittieren.

> ***"It is quite easy to find devices that use Samba in Shodan: searching for port 445 with a 'samba' string will turn up a viable IP list. An attacker would then simply need to create a tool that can automatically write malicious files to every IP address on the list."***
> **– TrendMicro-Bericht**

Was genau die Angreifer mit den erbeuteten NAS-Boxen machen, sagt TrendMicro nicht – es ist aber aller Wahrscheinlichkeit nach nichts gutes. Sie könnten es vor allem auf die auf den Geräten gespeicherten Daten abgesehen haben. Diese sind ein lohnendes Ziel für Spionageangriffe oder Erpressungstrojaner.

Die Hacker scheinen immerhin keine Probleme zu haben, Ziele zu finden. "Es ist recht einfach, Geräte die Samba benutzen in Shodan zu finden. Ein Angreifer muss dann nur noch ein Tool schreiben, welches bösartige Dateien automatisch auf alle Ziel-IPs von dieser Liste schreibt", erläutern die Sicherheitsforscher. Shodan ist eine Suchmaschine, die es erlaubt, öffentlich erreichbare Endpunkte im Netz anhand bestimmter Ports oder Protokolle zu finden.

Für viele Geräte gibt es wenig Hoffnung

Zwar hat so ziemlich jede Linux-Distribution die SambaCry-Lücke mittlerweile geschlossen, da es sich bei den meisten NAS-Geräten allerdings um Embedded-Systeme handelt, sind viele von ihnen noch angreifbar. Hier zeigt sich wieder einmal das alte Problem mit dem Internet der Dinge (Internet of Things, IoT) und Herstellern, welche die Firmware auf ihren Geräten nur sehr langsam und in den meisten Fällen gar nicht aktualisieren. So wie es aussieht wird uns auch die SambaCry-Lücke noch auf Jahre Angriffe bescheren, die diese Schwachstelle missbrauchen. (fab)

Kommentare lesen (344 Beiträge)

Forum zum Thema: **Serversicherheit**

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

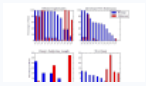
heise devSec

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.

https://heise.de/-3777456 Drucken

Mehr zum Thema **Sicherheitslücken** **Samba** **SMB** **Internet der Dinge** **NAS** **Linux und Open Source**

Neueste Forenbeiträge

Re: Aber nur wenn das NAS von aussen erreichbar

Stecknadel schrieb am 20.07.2017 13:03: Was heißt "sind frei"? Defaultmäßig sind die im Router ganz sicher nicht freigeschaltet, wie sollte das…

Forum: SambaCry: Erste Angriffe auf Linux-NAS-…

von ErzlordCaron; 20.07.2017 14:27

Re: Nö.

Selbst gebasteltes System sollte kein Problem sein. Namhafte Hersteller die auch vernünftig Updates veröffentlichen sind auch ok. Problematisch…

Forum: SambaCry: Erste Angriffe auf Linux-NAS-…

von Troeterich; 20.07.2017 14:27

Workaround ? Einfach stecker ziehen!

Also einfach Daten retten und das Gerät entsorgen. Nächtest mal eig. Server zusammen bauen.

Forum: SambaCry: Erste Angriffe auf Linux-NAS-…

von cytron; 20.07.2017 14:25

Der Kommentar

1 2 3 4 5

Politische Lösungen für eine sichere Zukunft der Kommunikation

Nach den Snowden-Enthüllungen steht eine Diskussion an, was wir zukünftig besser machen können, um Spionage und großflächige Massenüberwachung zu verhindern. Neben besserer Technik braucht es da auch neue politische Ansätze, meint Linus Neumann.

Copyright © 2017 Heise Medien Content Management by InterRed