heise Security

Sicherheitsupdate in Sicht: Gravierende Telnet-Lücke bedroht zahlreiche Cisco-Switches

Alert! 20.03.2017 11:20 Uhr
Dennis Schirrmacher

(Bild: dpa, Felix Kästle/Illustration)

Offensichtlich hat Cisco den Vault-7-Leak analysiert und ist auf eine kritische Lücke in über 300 Modellen seiner Switch-Reihe mit IOS-Betriebsystem gestoßen. Bislang gibt es nur einen Workaround - ein Patch soll folgen.

Ciscos Cluster Management Protocol (CMP) ist verwundbar. Das Protokoll kommt im IOS- und IOS-XE-Betriebssystem zum Einsatz. Insgesamt sollen über 300 verschiedene Switch-Modelle des Herstellers von der als äußerst kritisch eingestuften Lücke bedroht sein. Die betroffenen Geräte listet der Hersteller **in seiner Warnmeldung[1]** auf. Diese sind Cisco zufolge bereits in der Standardkonfiguration gefährdet.

Nutzen Angreifer die Lücke aus, sollen sie aus der Ferne und ohne Authentifizierung Schadcode ausführen können. Über diesen Weg kapern Angreifer in der Regel ganze Geräte. Cisco vergibt für die Schwachstelle einen CVSS 3.0 Score von 9.8 von maximal 10 Punkten.

Das Kapern von Switches ist besonders gefährlich, weil diese das Rückgrat einer Firmen-Netzwerkstruktur bilden. Wenn man diese Geräte kontrolliert, kann man sich im Firmennetz sehr weit ausbreiten – ungehindert von virtuellen Grenzen, wie sie etwa VLANs darstellen.

Gefährliche Telnet-Verbindung

CMP setzt auf das Netzwerkprotokoll Telnet, um lokal in einem Cluster zu kommunizieren. Das Problem dabei ist, dass in diesem Kontext offenbar auch Telnet-Verbindungen nach außen aufgebaut werden können. Dafür müssen Angreifer lediglich präparierte Telnet-Anfragen an das CMP schicken, was diese akzeptiert, führt Cisco aus.

Bislang hat Cisco einen Sicherheitspatch nur angekündigt, aber noch nicht veröffentlicht. Bis dahin empfiehlt der Hersteller Telnet auf betroffenen Geräte zu deaktivieren und bis zum Erscheinen des Patches auf SSH zu setzen.

Die Lücke stammt aus den Dokumenten des Vault-7-Leaks. Darin finden sich zum Beispiel Zero-Day-Lücken, die die CIA für ihre Arbeit ausgenutzt haben soll. (**des[2]**)

URL dieses Artikels:

`http://www.heise.de/-3658915`

Links in diesem Artikel:

[1] `https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp`

[2] `mailto:des@heise.de`

Copyright © 2017 Heise Medien

...