ADAM121 - FOTOLIA

Leaked Cisco security vulnerability found in NSA exploit stockpile

by
Michael Heller
Senior Reporter

Published: 23 Aug 2016

A Cisco security vulnerability affecting routers was found in the Shadow Brokers cyberweapon dump and may have been used by the NSA for years to decrypt VPN traffic.

THIS ARTICLE COVERS

Network Firewalls, Routers and Switches

LOOKING FOR SOMETHING ELSE?

Juniper firewall backdoors add fuel to encryption debate
Cisco router malware in the wild more widespread than first believed
Cisco IOS security patches address denial-of-service vulnerabilities

+ Show More

A researcher found an exploit in the dump of NSA-linked cyberweapons which abuses a Cisco security vulnerability and highlights the dangers of using hardware that is no longer supported by the manufacturer.

The exploit, called BENIGNCERTAIN, revealed by Mustafa Al-Bassam, former black hat hacker and current security researcher, is a remote exploit for the Cisco PIX router which could allow an attacker to decrypt the VPN traffic passing through the device. The exploit was found in the dump of Equation Group exploits said to include a stockpile of NSA cyberweapons.

According to Al-Bassam, the exploit "sends an Internet Key Exchange packet to the victim machine, causing it to dump some of its memory. The memory dump can then be parsed to extract an RSA private key and other sensitive configuration

information."

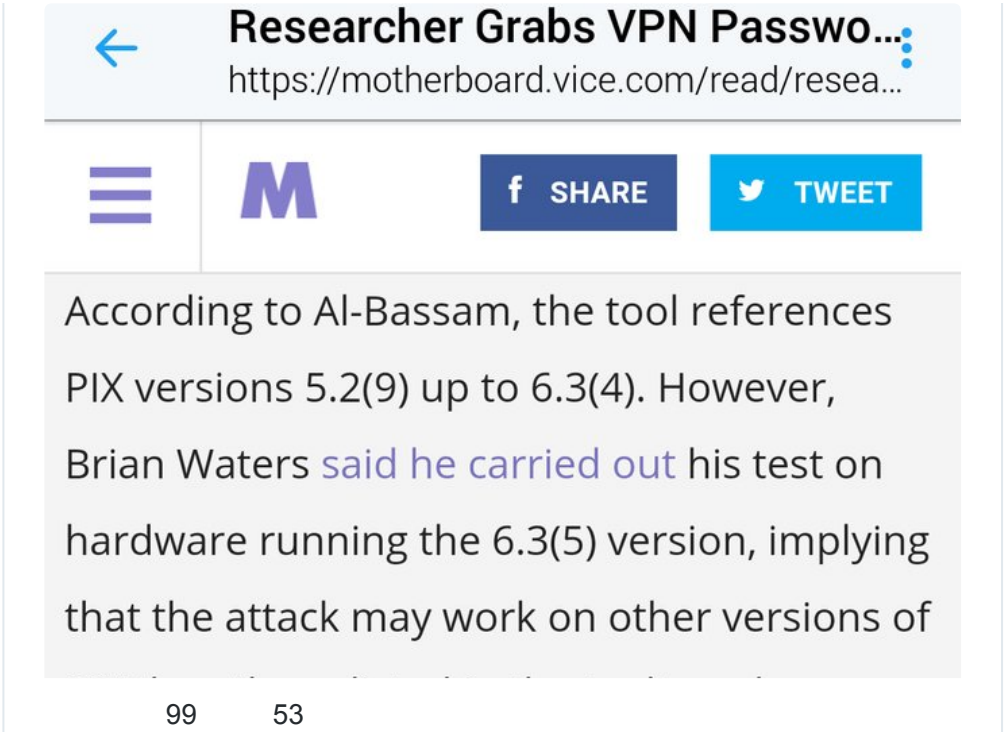
In his original blog post, Al-Bassam said the BENIGNCERTAIN tool referenced Cisco PIX versions 5.2(9) to 6.3(4), but later confirmed on Twitter that the Cisco security vulnerability was also present in PIX 6.3(5).

Mustafa Al-Bassam 19 Aug
@musalbas

BENIGNCERTAIN confirmed to remotely extract Cisco PIX VPN pre-shared key. Apparently works with unauthed attackers.
pic.twitter.com/mpaHp3hZ2D

Mustafa Al-Bassam Follow
@musalbas

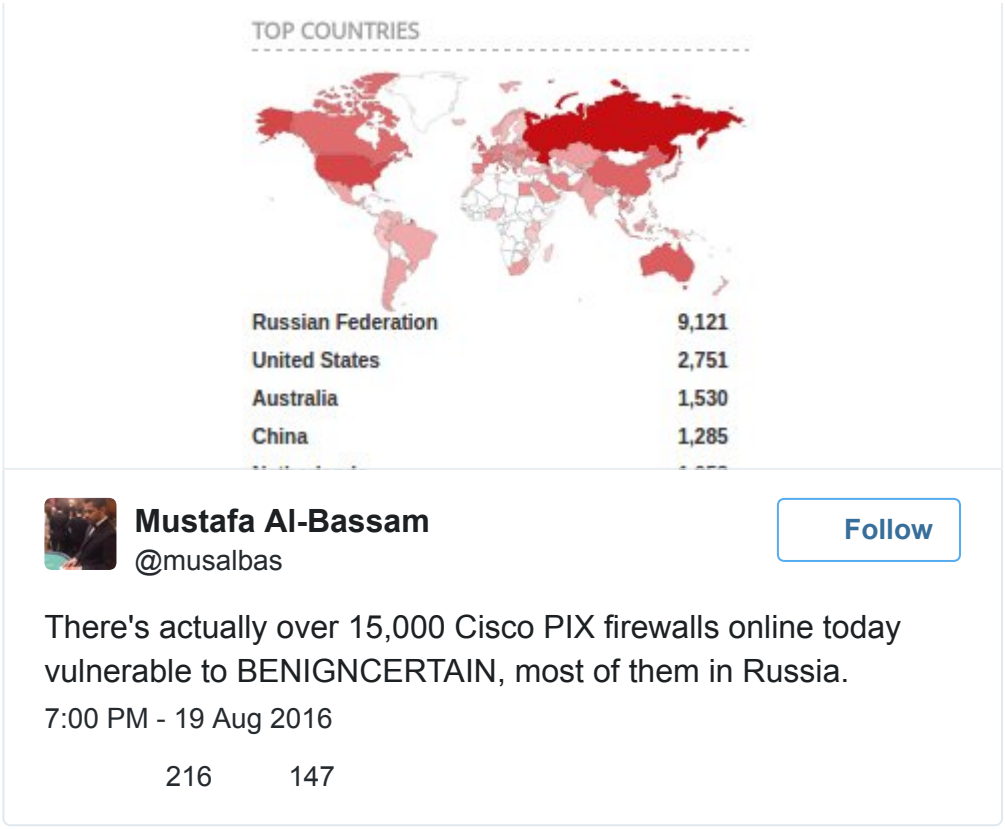
BENIGNCERTAIN works on PIX 6.3(5), meaning that the NSA was able to decrypt any Cisco VPN traffic from 2002 to 2008.
pic.twitter.com/x15vs5dSkW
2:29 PM - 19 Aug 2016



Omar Santos, principal engineer for the Cisco Product Security Incident Response Team (PSIRT), acknowledged the vulnerability in a blog post.

"Our investigation so far has not identified any new vulnerabilities in current products related to the exploit," Santos wrote. "Even though the Cisco PIX is not supported and has not been supported since 2009, out of concern for customers who are still using PIX we have investigated this issue and found PIX versions 6.x and prior are affected. PIX versions 7.0 and later are confirmed to be unaffected by BENIGNCERTAIN. The Cisco ASA is not vulnerable."

Al-Bassam noted Cisco ended support altogether for PIX version 6.3 in 2013, but there are still more than 15,000 vulnerable devices deployed in the wild.



Santos warned of the risks of using unsupported products.

"Just as technology advances, so too do the nature and sophistication of attacks," Santos wrote. "Prolonging the use of older technology exponentially increases risk."

Garve Hays, solutions architect for Micro Focus, told SearchSecurity that enterprises should not use unsupported products because they will be vulnerable.

"The concept of the 'long tail' applies to vulnerabilities as well, so it should come as no surprise that there is someone out there still using something they probably shouldn't," Hays said. "Given that notion, in this case Cisco actively provided

patches well into 2009, so there is no excuse for not keeping their appliances patched and up to date. In general, an organization should presume they are vulnerable and follow a process that includes policy, review, and remediation."

Hays also noted it is likely that the NSA wasn't the only actor with this exploit.

"Cisco is a high value target for many actors, so it is likely that others are cognizant of it and have used the exploit," Hays said. "In my opinion the NSA should have disclosed the flaw to Cisco. That is at the very heart of responsible disclosure."

Rebecca Herold, CEO of Privacy Professor, agreed the NSA should have disclosed the Cisco security vulnerability.

"Given the huge vulnerability and exposure to everyone using these specific types of PIX firewalls, yes, they definitely should have [disclosed it]. Especially for technology that was created specifically to be used for security purposes, and is being widely used by huge organizations, which have the data of millions of individuals," Herold told SearchSecurity via email. "Failure to notify a security technology vendor of a security flaw, and indeed even to exploit it and use it for their own purposes for many years is quite frankly unethical and diametrically opposed to the NSA's mission to 'defend vital networks.' The NSA claims to be doing surveillance in the name of security, when their very actions have put the security of all those using the affected PIX firewalls at very real risk."

Michael Heller asks:

What do you think of the NSA stockpiling Cisco security vulnerabilities?

[redacted]

0 Responses

Join the Discussion

Next Steps

Learn more about the fallout from the Equation Group cyberweapons leak.

Find out how Juniper firewall backdoors added fuel to the encryption debate.

Get info on the risks of using unsupported software.

Dig Deeper on Network Firewalls, Routers and Switches

ALL | NEWS | GET STARTED | EVALUATE | MANAGE | PROBLEM SOLVE

Aruba RFProtect WIPS: Product overview

Cisco Adaptive Wireless IPS: Product overview

Check Point Next Generation Firewall: Product overview

Cisco ASA with FirePOWER: NGFW product overview

Load More

0 comments

Oldest ▼

Share your comment

Send me notifications when other members comment.

Register or Login

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

Latest TechTarget resources

CLOUD SECURITY

NETWORKING

CIO

CONSUMERIZATION

SearchCloudSecurity

How the cloud can help organizations with security log data

Organizations often have to deal with copious amounts of security log

data and that can be challenging. Expert Frank Siemons ...

DDoS mitigation services: What to consider before implementation

Before implementing DDoS mitigation services, there are a few things enterprises should consider. Expert Ed Moyle discusses the ...