RISK ASSESSMENT —

NSA-linked Cisco exploit poses bigger threat than previously thought

With only a small amount of work, ExtraBacon will commandeer new versions of ASA.

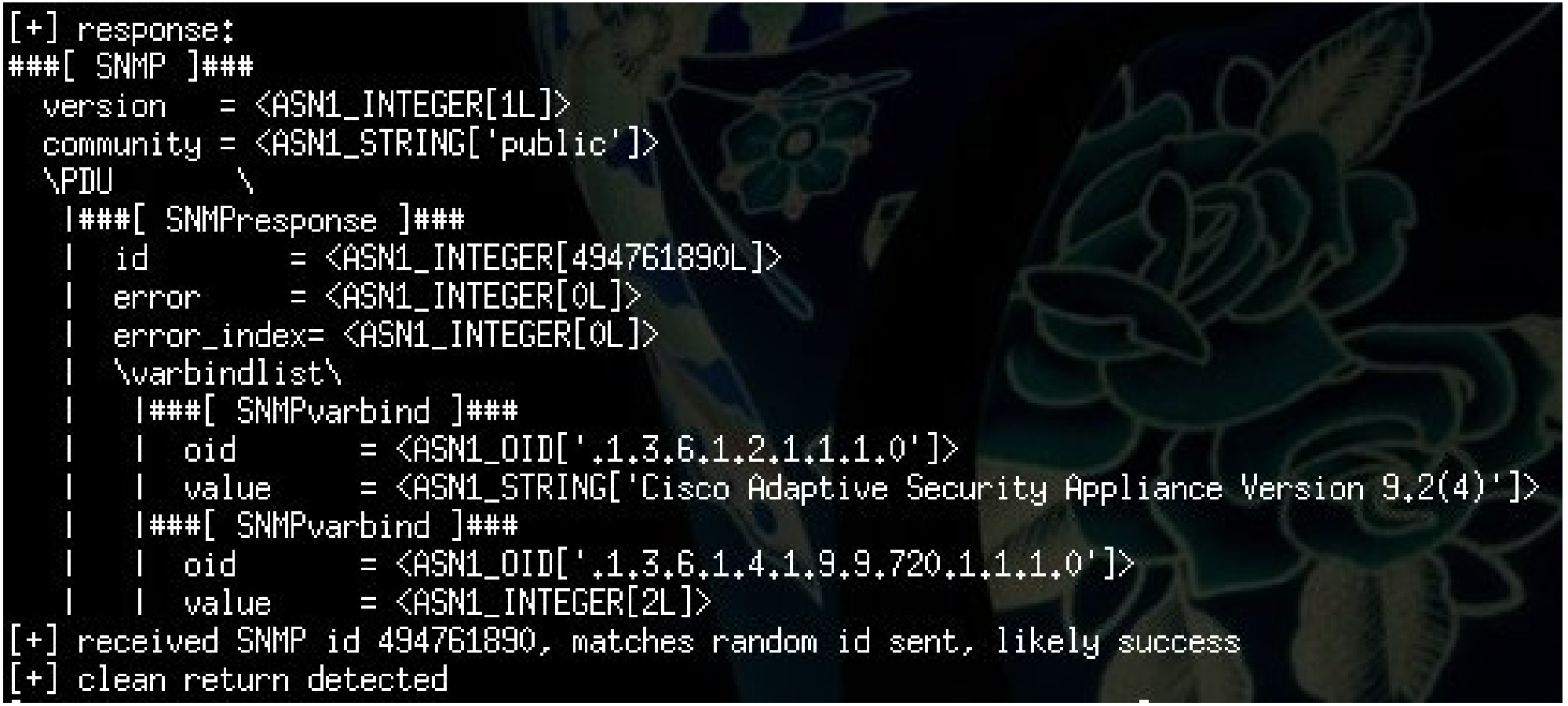
DAN GOODIN - 8/23/2016, 8:09 PM

Enlarge

46

Recently released code that exploits Cisco System firewalls and has been linked to the National Security Agency can work against a much larger number of models than many security experts previously thought.

An exploit dubbed ExtraBacon contains code that prevents it from working on newer versions of Cisco Adaptive Security Appliance (ASA), a line of firewalls that's widely used by corporations, government agencies, and other large organizations. When the exploit encounters 8.4(5) or newer versions of ASA, it returns an error message that prevents it from working. Now researchers say that with a nominal amount of work, they were able to modify ExtraBacon to make it work on a much newer version. While Cisco has said all versions of ASA are affected by the underlying vulnerability in the Simple Network Messaging Protocol, the finding means that ExtraBacon poses a bigger threat than many security experts may have believed.



SilentSignal

The newly modified exploit is the work of SilentSignal, a penetration testing firm located in Budapest, Hungary. In an e-mail, SilentSignal researcher Balint Varga-Perke wrote:

> We first started to work on the exploit mainly to see how easy it would be to add support for other (newer) versions. Turns out it is very easy, that implies two things:
>
> - The leaked code is not as poor quality as some might suggest
> - The lack of exploit mitigation techniques in the target Cisco software makes the life of attackers very easy

As zero-day exploit allows remote attackers who have already gained a foothold in a

FURTHER READING

targeted network to take full control of a firewall. It was one of more than a dozen highly advanced attacks that was part of a mysterious leak by a previously unknown group calling itself the ShadowBrokers. Researchers say digital fingerprints left inside the code all but prove the attacks belonged to the Equation Group, an elite hacking crew with ties to the NSA-sponsored Stuxnet and Flame malware that targeted Iran and the Middle East.

Cisco confirms NSA-linked zeroday targeted its firewalls for years

Michael Toecker, an engineer at a firm called Context Industrial Security, has analyzed ExtraBacon and found that it was designed to work only with versions 8.4(4) and earlier of ASA. He provided the following screenshot to illustrate the restrictions.

extrabacon_1.1.0.1.py

```
118             return "asa804-32"
119         elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(5)":
120             return "asa805"
121         elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(1)":
122             return "asa821"
123         elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(2)":
124             return "asa822"
125         elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(3)":
126             return "asa823"
127         elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(4)":
128             return "asa824"
129         elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(5)":
130             return "asa825"
131         elif vers_string == "Cisco Adaptive Security Appliance Version 8.3(1)":
132             return "asa831"
133         elif vers_string == "Cisco Adaptive Security Appliance Version 8.3(2)":
134             return "asa832"
135         elif vers_string == "Cisco Adaptive Security Appliance Version 8.4(1)":
136             return "asa841"
137         elif vers_string == "Cisco Adaptive Security Appliance Version 8.4(2)":
138             return "asa842"
139         elif vers_string == "Cisco Adaptive Security Appliance Version 8.4(3)":
140             return "asa843"
141         elif vers_string == "Cisco Adaptive Security Appliance Version 8.4(4)":
142             return "asa844"
143         else:
144             return "unsupported"
```

Michael Toecker

Th

slit" demonstrates just how persistent a vulnerability in code can be, how it

FURTHER READING

moves into new versions unless it's found and eradicated," Toecker told Ars. "I don't know who built ExtraBacon, but thousands of users in the US are now vulnerable to the same exploit because nobody told Cisco their SNMP code was busted, and the vulnerable code continued into later versions."

How “omnipotent” hackers tied to NSA hid for 14 years—and were found at last

Toecker went on to say that the vulnerability of later ASA versions likely didn't take Cisco by surprise. Near the bottom of a post that Cisco published last week in response to the ShadowBrokers leak, the company's principal engineer, Omar Santos, reported that ExtraBacon caused ASA version 9.4(1) to seize up and stop working. Such crashes are often the first sign of a bug that, when properly exploited, allows an attacker to remotely execute malicious code.

Cisco engineers have released software that allows ASA customers to detect and stop ExtraBacon-powered attacks, but the company has yet to actually patch the underlying bug. The ShadowBrokers release means that advanced attacks can be carried out by a much wider base of hackers than would normally be possible.

"We have test equipment and custom firmware images that make debugging easier," Varga-Perke of SilentSignal said. "These are most likely available for malicious parties, too; we are quite confident that similar code exists in private hands."

As Ars and Cisco have noted previously, the ExtraBacon exploit requires attackers to already have compromised parts of a targeted network. That requirement and the bar Varga-Perke described for modifying ExtraBacon means it's probably prohibitively difficult for script kiddies to exploit newer versions of ASA. Still, for more talented hackers, there's no longer any debate. People running ASA should make sure they've installed last week's exploit signature and the upcoming patch as soon as it's available.

I bet there's a much newer version of that tool somewhere in Equation's coffers, with a much expanded list of ASA versions it'll allow itself to run on.

581 posts | registered 10/29/2014

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 46

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

SIGN IN