ars TECHNICA

RISK ASSESSMENT —

Cisco confirms NSA-linked zeroday targeted its firewalls for years

Company advisories further corroborate authenticity of mysterious Shadow Brokers leak.

DAN GOODIN - 8/17/2016, 6:35 PM

Cisco Systems has confirmed that recently-leaked malware tied to the National Security Agency exploited a high-severity vulnerability that had gone undetected for years in every supported version of the company's Adaptive Security Appliance firewall.

The previously unknown flaw makes it possible for remote attackers who have already gained a foothold in a targeted network to gain full control over a firewall, Cisco warned in an advisory published Wednesday. The bug poses a significant risk because it allows attackers to monitor and control all data passing through a vulnerable network. To exploit the vulnerability, an attacker must control a computer already authorized to access the firewall or the firewall must have been misconfigured to omit this standard safeguard.

"It's still a critical vulnerability even though it requires access to the internal or management network, as once exploited it gives the attacker the opportunity to monitor all network traffic," Mustafa Al-Bassam, a security researcher, told Ars. "I wouldn't imagine it would be difficult for the NSA to get access to a device in a large company's internal network, especially if it was a datacenter."

All the more menacing

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

The vulnerability, which Cisco rated as "high," is all the more menacing given the release over the weekend of hacking tools that have been all but definitively linked to Equation Group, an elite hacking team with ties to the NSA that remained hidden for more than 14 years. With the release of professionally developed code that exploits the Cisco vulnerability, attacks can now be carried out by a much larger base of hackers.

The weaponized attack exploited a vulnerability residing in Cisco's implementation of the Simple Network Management Protocol. The exploit was the engine behind "ExtraBacon," one of 15 distinct pieces of attack code included in the still-mysterious leak from last weekend. A blog post from Tuesday demonstrated how ExtraBacon allowed an unauthenticated person to take control of Adaptive Security Appliance firewalls. Cisco's confirmation now suggests that people within the US government have known of the risk since at least 2013 and allowed it to persist.

Cisco has yet to actually patch the vulnerability, which is indexed as CVE-2016-6366. Instead, the company is releasing signatures that can detect the exploits and stop them before they allow an attacker to seize control of vulnerable networks. Another workaround is to disable SNMP altogether. A Cisco representative said the company will release a patch in the near future. Cisco said a separate piece of attack code dubbed EpicBanana exploited a different, already fixed vulnerability in the same line of firewalls. The medium-severity flaw, indexed as CVE-2016-6367, was patched in 2011, but in keeping with Cisco practices at the time, it wasn't assigned its own vulnerability designation because of the relatively low severity rating, a company representative told Ars. According to Cisco's advisory, it "could allow an authenticated, local attacker to create a denial of service (DoS) condition or potentially execute arbitrary code." Cisco also provided this overview on Shadow Brokers, the previously unknown group that published the exploits.

Separately, Cisco competitor Fortinet disclosed a high-severity vulnerability in older security devices it sells. "FortiGate firmware (FOS) released before Aug 2012 has a cookie parser buffer overflow vulnerability," the notice warned. "This vulnerability, when exploited by a crafted HTTP request, can result in execution control being taken over." The previously mentioned catalog of leaked exploits shows that the vulnerability was exploited by malware known as EgregiousBlunder. FortiGate's advisory said it continues to investigate whether other company products are vulnerable.

More shoes to drop?

With confirmations from Cisco and Fortinet that their products were directly targeted by the leaked exploits, security researchers are now turning their attention to Juniper, whose NetScreen line of firewalls are also mentioned in the catalog. It's possible the exploit relies on a previously disclosed backdoor that was the result of "unauthorized code" that managed to remain hidden for years in NetScreen. The backdoor allowed attackers to decrypt encrypted traffic passing over virtual private networks used by Juniper customers. So far, Juniper representatives haven't responded to questions.

With more than a dozen cataloged exploits still unaddressed, it wouldn't be surprising to see similar disclosures and advisories in the coming days or weeks. People who rely on any of the affected products mentioned in the Shadow Brokers exploits should be prepared to work overtime and may want to consider shutting down unneeded services as a precaution.

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