Threatpost | The first stop for security news

- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - The Kaspersky Lab News Service

Featured Posts

All

 GPG Patches 18-Year-Old Libgcrypt RNG Bug

 Locky Targets Hospitals In Massive Wave…

 Unsecured DNSSEC Easily Weaponized, Researchers Warn

 Gunter Ollmann on the Future of…

 Apple Launches Bug Bounty with Maximum…

 How Bugs Lead to a Better…

- Podcasts

Latest Podcasts

All

 Threatpost News Wrap, August 19, 2016

 Joshua Drake on Android Security Post-Stagefright

 Threatpost Black Hat Preview, August 2,...

 Threatpost News Wrap, July 29, 2016

 Threatpost News Wrap, July 15, 2016

 Threatpost News Wrap, July 8, 2016

Recommended

The Kaspersky Lab Security News Service

- Videos

Latest Videos

All

 Bruce Schneier on the Integration of...

Chris Valasek Talks Car Hacking, IoT,...

 Patrick Wardle on OS X Malware...

 Santiago Pontiroli and Roberto Martinez on...

 Dewan Chowdhury on Hacking Power Grids

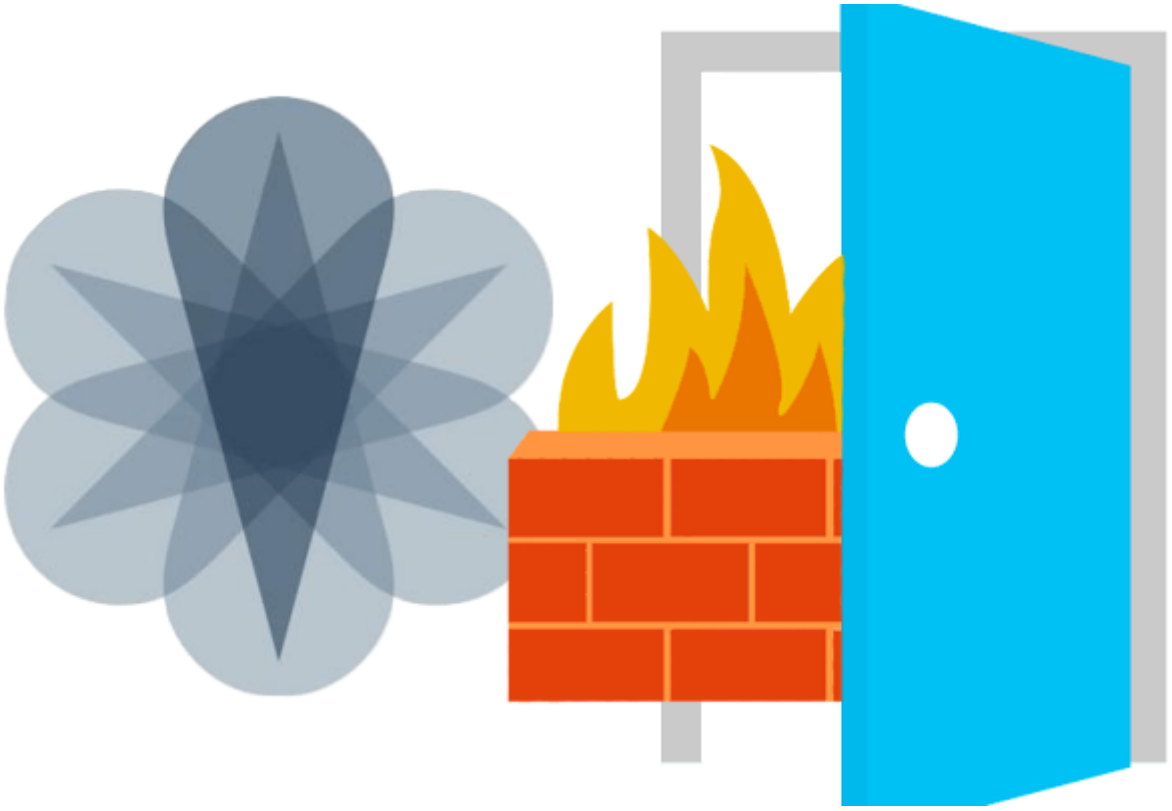
 Sergey Lozhkin on How He Hacked...

Recommended

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS



Juniper Acknowledges Equation Group Targeted ScreenOS

Follow @mike_mimoso by Michael Mimoso August 22, 2016 , 1:52 pm

Juniper Networks on Friday acknowledged that ~~exploits~~ implants contained in the ShadowBrokers data dump do indeed target its products.

“As part of our analysis of these files, we identified an attack against NetScreen devices running ScreenOS,” said Derrick Scholl, director of security incident response at Juniper. “We are examining the extent of the attack, but initial analysis indicates it targets the boot loader and does not exploit a vulnerability on ScreenOS devices.”

Related Posts

Threatpost News Wrap, August 19, 2016

August 19, 2016 , 9:00 am

OIG Report Finds Vulnerabilities in Medicaid Services Agency

August 18, 2016 , 12:55 pm

Cisco Acknowledges ASA Zero Day Exposed by ShadowBrokers

August 17, 2016 , 4:06 pm

“We will continue to evaluate exactly what level of access is necessary in order to execute the attack, whether it is possible to detect the attack, and if other devices are susceptible,” Juniper’s Scholl said.

Exploits for vulnerabilities in Cisco and Fortinet products were also exposed in the data dump by the still-unidentified members of the ShadowBrokers, who last week kicked off an auction of exploits belonging to the so-called Equation Group, largely believed to be affiliated with the National Security Agency.

The Equation Group is considered to be at the top of the APT food chain. A number of researchers, including those at Kaspersky Lab who uncovered and in 2015 reported on the cyberespionage group, confirmed strong connections between the exploits and previous attack tools alleged to belong to the group.

Juniper is the last among the three giant networking vendors targeted by the Equation Group to acknowledge the legitimacy of the files. Cisco, last week, said that one of the attacks targets a zero-day vulnerability in its ASA firewall that has yet to be patched. Another in the ASA command-line interface parser was patched in 2011; that bug could crash appliances running the software allow for code execution if an attacker was already on the machine, Cisco said.

The Cisco zero-day, meanwhile, is in ASA’s SNMP implementation that could allow an unauthenticated remote attacker to remotely execute code on the box. Cisco said it has released an IPS signature, Legacy Cisco IPS Signature ID: 7655-0, and a Snort rule, ID: 3:39885.

“The vulnerability is due to a buffer overflow in the affected code area. An attacker could exploit this vulnerability by sending crafted SNMP packets to the affected system,” Cisco said in its advisory. “An exploit could allow the attacker to execute arbitrary code and obtain full control of the system or to cause a reload of the affected system. The attacker must know the SNMP community string to exploit this vulnerability.”

Late last week, researcher Mustafa Al-Bassam tackled a another Equation Group exploit in the dump called BENIGNCERTAIN. This one targets Cisco PIX firewalls that are no longer supported by the company. The attack, Al-Bassam said, allows attackers to remotely sniff and steal private RSA encryption keys.

“Analysis of the tool shows that it appears to be a remote exploit for Cisco PIX devices that sends an Internet Key Exchange (IKE) packet to the victim machine, causing it to dump some of its memory,” Al-Bassam wrote in his report. “The memory dump can then be parsed to extract an RSA private key and other sensitive configuration information.”

Cisco, on Friday, responded to this attack as well saying that its investigation into BENIGNCERTAIN has not turned up any new vulnerabilities in current products.

“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,” Cisco’s Omar Santos wrote in an updated ShadowBrokers advisory. “PIX versions 7.0 and later are confirmed to be unaffected by BENIGNCERTAIN. The Cisco ASA is not vulnerable.”

As for Juniper’s acknowledgement, this isn’t the first time its enterprise gear has been targeted by the NSA. Its products were singled out in NSA documents taken by whistleblower Edward Snowden and published by Der Spiegel in 2013. Late last year, the company said it found and removed “unauthorized code” from its ScreenOS operating system that allowed attackers to decrypt VPN traffic from NetScreen devices.

In the 2013 Der Spiegel article written by Jacob Appelbaum Judit Horchert and Christian Stocker, the authors described the NSA’s FEEDTHROUGH implant that provided backdoor access to NetScreen firewalls and VPNs running Screen OS. Two vulnerabilities were found and patched last December by Juniper, one being the VPN decryption backdoor, and another that allowed from remote access to NetScreen devices over SSH or telnet.

Categories: Government, Hacks, Vulnerabilities

Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite="">`

<cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike>

Name

Email

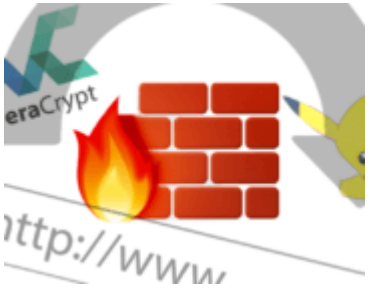
I'm not a robot
reCAPTCHA
Privacy - Terms

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Recommended Reads



0 3 21 0 0

August 19, 2016 , 9:00 am
Categories: Cryptography, Government, Mobile Security, Podcasts, Privacy, Vulnerabilities

Threatpost News Wrap, August 19, 2016

by Chris Brook

Mike Mimoso and Chris Brook discuss the news of the week, including the Shadow Brokers debacle, the VeraCrypt audit, Pokemon ransomware, and a browser address bar vulnerability.

Read more...

0 7 15 0 0

August 18, 2016 , 12:55 pm
Categories: Government, Vulnerabilities

OIG Report Finds Vulnerabilities in Medicaid Services Agency

by Chris Brook

Vulnerabilities in Centers for Medicare & Medicaid Services could result in the disclosure of personally identifiable information and the “disruption of critical operations,” a government watchdog warned this week.

Read more...

0 8 243 0 1

August 17, 2016 , 4:06 pm
Categories: Government, Vulnerabilities, Web Security

Cisco Acknowledges ASA Zero Day Exposed by ShadowBrokers

by Michael Mimoso

Cisco today acknowledged two vulnerabilities in its Adaptive Security Appliance that were leaked in the ShadowBrokers data dump of Equation Group exploits.

Read more...

Top Stories

Threatpost News Wrap, August 19, 2016

August 19, 2016 , 9:00 am

Cisco Acknowledges ASA Zero Day Exposed by ShadowBrokers

August 17, 2016 , 4:06 pm

Pokémon GO Spam, Ransomware, On the Rise

August 17, 2016 , 12:58 pm

ProjectSauron APT On Par With Equation, Flame, Duqu

August 8, 2016 , 1:40 pm

Miller, Valasek Deliver Final Car Hacking Talk

August 4, 2016 , 3:26 pm

Researchers Go Inside a Business Email Compromise Scam

August 4, 2016 , 10:00 am

Export-Grade Crypto Patching Improves

August 3, 2016 , 10:00 am

Kaspersky Lab Launches Bug Bounty Program

August 2, 2016 , 9:00 am

Threatpost News Wrap, July 29, 2016

July 29, 2016 , 10:45 am

KeySniffer Vulnerability Opens Wireless Keyboards to Snooping

July 26, 2016 , 9:30 am

Upcoming Tor Design Battles Hidden Services Snooping

July 25, 2016 , 3:51 pm

EFF Files Lawsuit Challenging DMCA's Restrictions on Security Researchers

July 21, 2016 , 1:18 pm

Oracle Patches Record 276 Vulnerabilities with July Critical Patch Update

July 20, 2016 , 9:21 am

Threatpost News Wrap, July 15, 2016

July 15, 2016 , 11:00 am

Academics Build Early-Warning Ransomware Detection System

July 14, 2016 , 1:05 pm

xDedic Hacked Server Market Resurfaces on Tor Domain

July 12, 2016 , 11:40 am

Conficker Used in New Wave of Hospital IoT Device Attacks

June 30, 2016 , 11:48 am

655,000 Healthcare Records Being Sold on Dark Web

June 28, 2016 , 10:00 am

Windows Zero Day Selling for $90,000

May 31, 2016 , 5:44 pm

Millions of Stolen MySpace, Tumblr Credentials Being Sold Online

May 31, 2016 , 1:37 pm

OTR Protocol Patched Against Remote Code Execution Flaw

March 10, 2016 , 10:23 am

Android KeyStore Encryption Scheme Broken, Researchers Say

July 7, 2016 , 11:52 am

Planes, Trains and Automobiles Increasingly in Cybercriminal's Bullseye

June 29, 2016 , 8:19 am

Hancitor Downloader Shifts Attack Strategy

August 22, 2016 , 2:27 pm

iOS 9.3.4 Patches Critical Code Execution Flaw

August 8, 2016 , 9:00 am

Apple Leaves iOS 10 Beta Kernel Unencrypted: Pros and Cons

June 27, 2016 , 5:13 pm

Voter Database Leak Exposes 154 Million Sensitive Records

June 24, 2016 , 10:14 am

Two Million Passwords Breached in Ubuntu Hack

July 18, 2016 , 1:17 pm

Popular Anime Site Infected, Redirecting to Exploit Kit, Ransomware

June 24, 2016 , 7:00 am

The Final Say

From Kaspersky Blogs

Weekend Volcano....

Volcanism. It’s one of my hobbies. I just love getting up volcanoes all over the planet. Something about their beauty, power, hooliganism, infamy, aliveness, hotness, lava, craters, calderas, la...

Read more...

[Threat intelligence report for the telecommunicati...]

The telecoms sector is under fire on all sides – hit by direct attacks on organizations and networks, indirect attacks in search of subscribers, and collateral damage from unrelated, targeted campaign...

Read more...

[The dark side of facial recognition technology]

Lynch law, loss of basic privacy, disgusting marketing, digital identity theft — how else can facial recognition be misused?

Read more...

Removing the barriers to mobile banking adoption

Mobile banking is easy and convenient, but its adoption rate is still far from ideal.

Read more...

Kaspersky Academy attended MIT (IC)3 Annual Confer...

72 guests, among them a global security lead Gordon Morrison, attended the MIT (IC)3 Annual Conference to share the latest insights into the industry. Educational programs manager Christel Gampig-Avil...

Read more...

Authors

Michael Mimoso
Tom Spring
Christopher Brook