PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Threat and vulnerabilities

Cisco, Fortinet issue patches against NSA malware

Undocumented SNMP string exposes Rockwell PLCS to remote attacks

Malware

Starwood, Marriott, Hyatt, IHG hit by malware: HEI

Ransomware

Caught in a web: Ranchi surfers log in to e-ransom threats

Top story

Government websites fall victim to virus attacks in Saudi Arabia

pwc

Cisco, Fortinet issue patches against NSA malware

Customers of certain Cisco and Fortinet security gear need to patch exploits made public this week after a purported hack of NSA malware.

Both companies have issued fixes to address exploits that were posted online and after they found the exploits represent real threats to some of their products, including versions of Cisco's popular PIX and ASA firewalls and versions of Fortinet's signature Fortigate firewalls.

Other exploits may affect Watchguard and TOPSEC products, but those companies did not immediately respond to inquiries. When they do this story will be updated. The exploits were posted as proof that a group called Shadow Brokers actually had in its possession malware that it claimed it hacked from the NSA.

While the exploits date from 2013 at the latest, Cisco says it just learned about one of them when Shadow Brokers made it public. Cisco already knew about a second one and had patched for it. Fortinet's lone security advisory is fresh.

Speculation is that Russia is behind releasing the exploits as a political move to blunt US reaction to Russia's alleged hack of the Democratic National Committee.

Cisco

Cisco rates the threat level of the newly discovered vulnerability – Cisco Adaptive Security Appliance SNMP Remote Code Execution Vulnerability – as high because it could allow execution of remote code on affected devices and obtain full control. "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," the advisory says.

Here is a list of the affected Cisco devices:

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco PIX Firewalls
- Cisco Firewall Services Module (FWSM)

The other vulnerability – Cisco ASA CLI Remote Code Execution Vulnerability – is one Cisco has known about since 2011 when it issued a fix for it. The company has issued a fresh security advisory for it in order to raise awareness so customers will make sure they've got software versions that patch the problem.

This vulnerability is ranked medium, and if exploited "could allow an authenticated, local attacker to create a denial of service (DoS) condition or potentially execute arbitrary code. An attacker could exploit this vulnerability by invoking certain invalid commands in an affected device," the advisory says.

Cisco has posted a blog that details its vulnerabilities and fixes.

Cisco, Fortinet issue patches against NSA malware

Fortinet

Fortinet has issued a security advisory for what it calls the Cookie Parser Buffer Overflow Vulnerability, whose importance it rates as high because it allows remote administrative access.

It affects certain Fortigate firmware called FOS released before August 2012. The affected versions are:

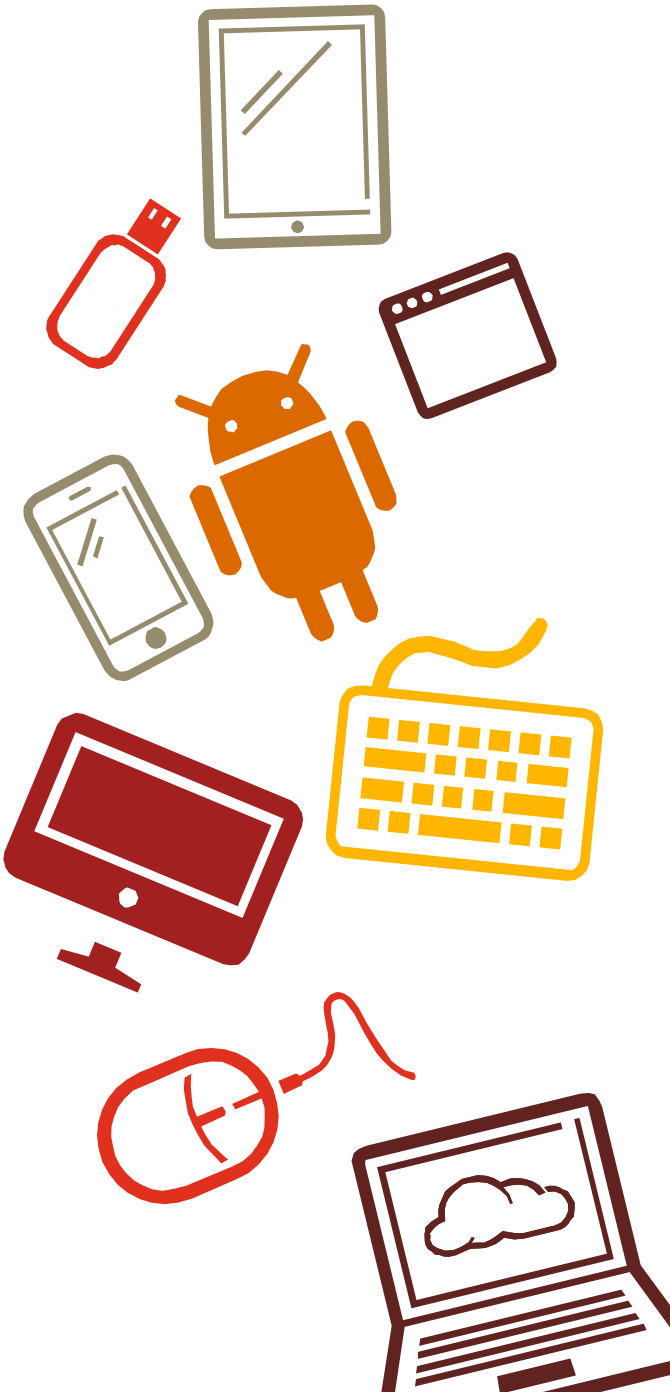
- FOS 4.3.8 and below
- FOS 4.2.12 and below
- FOS 4.1.10 and below

"Customers running FortiGate firmware 5.0 and above, released in August 2012 are not impacted," according to an emailed statement from Fortigate. "We continue to investigate this exploit and are conducting an additional review of all of our Fortinet products. If we identify any new information useful to our customers, we will share it through our responsible disclosure policy."

Source:
http://www.techcentral.ie/cisco-fortinet-issue-patches-against-nsa-malware/

Our perspective

Since both the OEMs have released a security advisory, we recommend verifying if they are affected and applying patches as per the procedure in the security advisory.



Undocumented SNMP string exposes Rockwell PLCS to remote attacks

An undocumented SNMP community string has been discovered in programmable logic controllers (PLCs) built by Allen-Bradley Rockwell Automation that exposes these devices deployed in a number of critical industries to remote attacks.

Researchers at Cisco Talos today said the vulnerability is in the default configuration of MicroLogix 1400 PLC systems. Rockwell Automation, meanwhile, said versions 1766-L32BWA, 1766-L32AWA, 1766-L32BXB, 1766-L32BWAA, 1766-L32AWAA, and 1766-L32BXBA are affected.

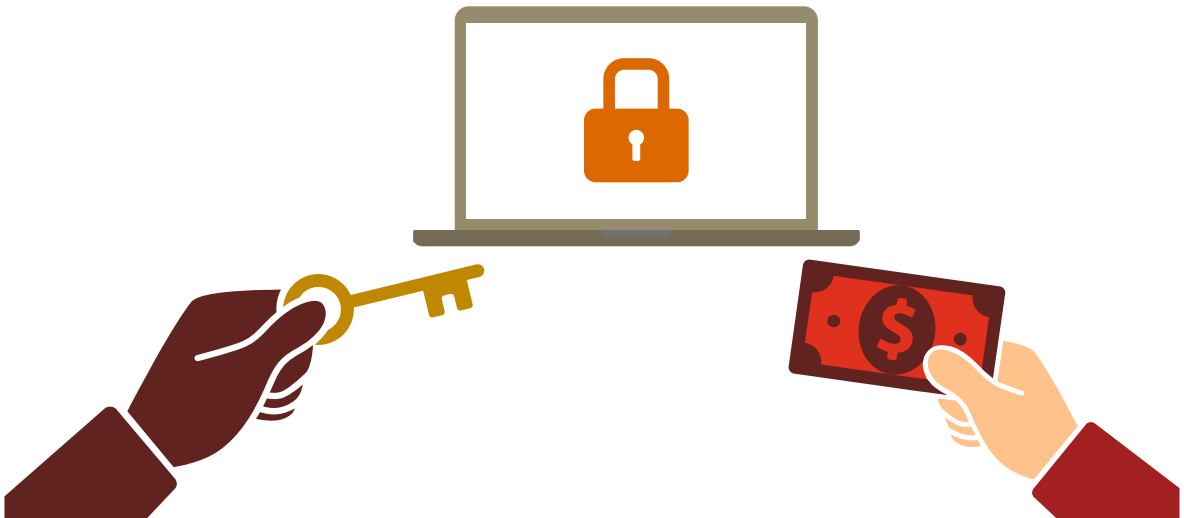
“This vulnerability is due to the presence of an undocumented SNMP community string that could be leveraged by an attacker to gain full control of affected devices and grants the ability to manipulate configuration settings, replace the firmware running on the device with attacker-controlled code, or otherwise disrupt device operations,” Cisco Talos wrote in an advisory. “Depending on the role of the affected PLC within an industrial control process, this could result in significant damages.”

According to an advisory published today by the Industrial Control System Cyber Emergency Response Team (ICS-CERT), these PLCs are used in industries such as chemical, manufacturing, food, water, wastewater and others across Europe, the United States and Asia. Cisco Talos said it also found an undocumented “wheel” string that also enabled read/write capabilities and exposes devices to unauthorized settings changes or firmware updates. Cisco cautions that the wheel string could also allow access to other object identifiers.

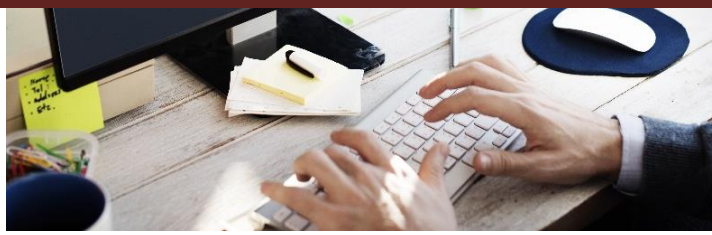
SNMP is a protocol used by many products for remote device management; in this case, for the deployment of firmware updates. “Due to the nature of this product’s firmware update process, this capability cannot be removed from the product,” ICS-CERT said in its advisory. Rockwell Automation provided a number of mitigations, including the use of a RUN keyswitch to prevent unauthorized firmware updates, and firewall updates to ensure SNMP requests from unauthorized sources are blocked.

“While it is possible for operators to change the default SNMP community strings on affected devices, the fact that this SNMP string is not documented by the vendor drastically decreases the likelihood of this value being changed prior to production deployment of the PLCs, as most operators are not likely to even be aware of its existence,” Cisco Talos said. “Given the severity of this issue, and the fact that this functionality has not been removed from affected devices, it is recommended that mitigations be put in place to prevent the successful exploitation of this vulnerability in production environments.”

Source:
https://threatpost.com/undocumented-snmp-string-exposes-rockwell-plcs-to-remote-attacks/119865/



Starwood, Marriott, Hyatt, IHG hit by malware: HEI



A data breach at 20 U.S. hotels operated by HEI Hotels & Resorts for Starwood, Marriott, Hyatt and Intercontinental may have divulged payment card data from tens of thousands of food, drink and other transactions, HEI said on Sunday.

The breach follows similar attacks at Hyatt Hotels Corp (H.N) and Starwood Hotels & Resorts Worldwide Inc (HOT.N) in recent months.

Norwalk, Connecticut-based HEI, which is privately held, said malware designed to collect card data was found on HEI's systems.

The malware was discovered in early to mid-June on payment systems used at restaurants, bars, spas, lobby shops and other facilities at the properties, Chris Daly, a spokesman for HEI, said in emails and phone calls.

The number of customers affected is difficult to calculate because they might have used their cards multiple times, Daly said. About 8,000 transactions occurred during the affected period at the Hyatt Centric Santa Barbara hotel in California, and about 12,800 at the IHG Intercontinental in Tampa, Florida, Daly said.

The malware affected 12 Starwood hotels, six Marriott International Inc (MAR.O) properties, one Hyatt hotel and one InterContinental Hotels Group PLC (IHG.L) hotel. It was active from March 1, 2015 to June 21, 2016, with 14 of the hotels affected after Dec. 2, 2015, HEI said on its website on Friday.

Marriott and IHG declined to comment. Representatives from the other hotel groups did not respond to requests for comment.

HEI said outside experts investigated the breach and determined that hackers might have stolen customer names, account numbers, payment card expiration dates and verification codes. The hackers did not appear to have gained PIN codes, since those are not collected by its system, it added.

The company has informed federal authorities and has installed a new payment processing system that is separate from other parts of its computer network.

Among the properties affected were Starwood's Westin hotels in Minneapolis; Pasadena, California; Philadelphia; Snowmass, Colorado; Washington, D.C.; and Fort Lauderdale, Florida. Also affected were Starwood properties in Arlington, Virginia; Manchester Village, Vermont; San Francisco; Miami; and Nashville, Tennessee.

The Marriott properties affected were in Boca Raton, Florida; Dallas-Fort Worth, Texas; Chicago; San Diego, California; and Minneapolis.

Source:
http://www.reuters.com/article/us-hotels-cyber-idUSKCN10P0ZM?rpc=401

Our perspective

Popular hotels in the US continue to be affected by data breaches in their payment systems. HEI has published FAQs for affected customers at http://www.heihotels.com/notice/2/ Digital payment systems are by nature extremely vulnerable and a continuous surveillance mechanism is required to ensure a safe and secure operating environment.

Caught in a web: Ranchi surfers log in to e-ransom threats

"Your computer has been infected with a virus. Click here to resolve the issue." "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine." "All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data."

If the above messages or any one among them looks familiar and you have seen them on your computer screen or smartphone, you must have been a victim of ransomware, one of the trending crimes recording a huge spurt in the cyber space recently. The modern form of extortion involves installation of malicious codes on the system covertly through lucrative and free downloads, encrypting of data and demanding a huge fees for its reversal.

Though appearing something very hi-tech for which the Federal Bureau of Investigation in the US and anti-virus companies like Kaspersky, McAfee and others have been burning their midnight oil has hit a small town like Ranchi. In less than a fortnight, more than three dozen cases of 'ransomware' extortion have been reported, though not in the open.

Till date, the victims have been automobile companies, one of the software consultants providing services to the government of Jharkhand, medical establishments and few small traders dealing in wholesale business. Most of them have received a timer on the home page of their respective 'computers or business workstation asking for certain amount of money to be paid in electronic form, failing which all data and details stored in the computers have threatened to be encrypted

"Though the security agencies related to enforcing cyber security in the state have remained tightlipped about the matter, founder president Cyber Peace Foundation, Vineet Kumar, who earlier helped Jharkhand police lay foundation of Cyber Defence Research Centre (CDRC), said during his Ranchi visit, he has got not less than a dozen walk-ins in his CPF office in the past one week. "To my knowledge, the maximum extortion that one of the victims in Ranchi was asked to pay was Rs 20 lakh, though this figure could be understated as the bitcoins are costly and mostly the extortionists direct the victims to pay through electronic money so that their identity and location remains discrete," he said.

So what's wrong if the data on any system is encrypted? Cyber experts clarify that in case of business and commercial activities such permanent loss of data and customer detail can lead to bankruptcy unless there is a backup data to restore the losses.

Sources in the CDRC of Jharkhand police admitted that certain complaints of smart phones being locked remotely have also reached them but in absence of technological knowhow formal cases have not been registered.

Source:

http://timesofindia.indiatimes.com/city/ranchi/Caught-in-a-web-Ranchi-surfers-log-in-to-e-ransom-threats/articleshow/53695334.cms

Government websites fall victim to virus attacks in Saudi Arabia

Jeddah-Some government agencies in Saudi Arabia have come under fierce virus attacks that aim at hacking their websites through sending spam messages to the inbox.

A government alert warned users in state agencies and mega companies of spam e-mails that might badly damage their computer devices. The alert added that hundreds of foreign addresses from diverse countries attacked websites of different government authorities; later on these websites functioned normally.

The official alert continued that the target user receives an e-mail with zipped folder attachments. Once the user downloads the five attachments, the virus spots the most important files on the computer and the virus is then activated.

Warnings added that there is also Boaxxe i.e. a backdoor that can be remotely controlled and can install, download and activate additives in famous web browsers such as Google, Firefox and Chrome.

Programmers said that hackers aim to cause the greatest damage possible through sending the user a full package virus on the electronic mail.

Experts forecast that more cyber-attacks on Middle East users are likely given that they basically depend on social network messages. Yet, they assured that careful check of the messages would foil any attempted attack.

This is the second time official websites get hacked and cyber-attacked from abroad in 2016. The Ministry of Interior was among the websites that stopped working during the past months.

In August 2015, Aramco was a victim of several cyber-attacks; Saudi authorities stated that these attacks aimed at halting production.

Source:

http://english.aawsat.com/2016/08/article55356795/government-websites-fall-victim-virus-attacks-saudi-arabia

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

MB/August2016-7227