(b)(3) 10 USC ⊥ 424

# [redacted] Cyber-Threat Newsletter – 09 Feb 16

*Patches & Updates of the Week:*

**(U) Cisco patches authentication, denial-of-service, and NTP flaws in many products**
Cisco Systems has released a new batch of security patches this week for flaws affecting a wide range of products, including for a critical vulnerability in its RV220W wireless network security firewalls. The RV220W vulnerability stems from insufficient input validation of HTTP requests sent to the firewall's Web-based management interface. This could allow remote unauthenticated attackers to send HTTP requests with SQL code in their headers that would bypass the authentication on the targeted devices and give attackers administrative privileges. Cisco has patched this vulnerability in the 1.0.7.2 firmware version for RV220W devices. Manual workarounds include disabling the remote management functionality or restricting it to specific IP addresses. The company also patched high- and medium-severity denial-of-service vulnerabilities in Cisco Wide Area Application Service (WAAS) appliances and modules, Cisco Small Business 500 Series switches and the SG300 managed switch. A cross-site scripting vulnerability was also patched in the Web-based management interface of Cisco Unity Connection. Finally, the company imported patches for 12 vulnerabilities in the Network Time Protocol daemon (ntpd) that were fixed on 19 January by the Network Time Foundation. These flaws can be exploited by attackers to modify the time on devices or to crash the ntpd process. The NTP flaws are suspected to affect over 70 Cisco products used for collaboration and social media products, network and security, routing and switching, unified computing and communications, streaming and transcoding, wireless and hosted services. The company has published firmware updates for some of them as well as a list of affected products and available patches that it will likely update as it releases more fixes. (IDG News Service, 29Jan16)

**(U) High-severity bug in OpenSSL allows attackers to decrypt HTTPS traffic fixed**
Maintainers of the OpenSSL cryptographic code library have fixed a high-severity vulnerability that made it possible for attackers to obtain the key that decrypts communications secured in HTTPS and other transport layer security channels. While the potential impact is high, the vulnerability can be exploited only when a variety of conditions are met. First, it's present only in OpenSSL version 1.0.2. Applications that rely on it must use groups based on the digital signature algorithm to generate ephemeral keys based on the Diffie Hellman key exchange. By default, servers that do this will reuse the same private Diffie-Hellman exponent for the life of the server process, and that makes them vulnerable to the key-recovery attack. DSA-based Diffie-Hellman configurations that rely on a static Diffie-Hellman ciphersuite are also susceptible. OpenSSL will now reject all key negotiations with Diffie-Hellman parameters shorter than 1,024 bits. A previous OpenSSL patch had increased the limit to 768 bits. People using OpenSSL version 1.0.2 should upgrade to 1.0.2f, while those still using version 1.0.1 should install 1.0.1r. Thursday's OpenSSL advisory also reminded users that support for version 1.0.1 will end at the end of this year, after which no security fixes will be available. Support for versions 0.9.8 and 1.0.0 ended in December. (ars technical, 28Jan16)

*Threats & Vulnerabilities of the Week:*

**(U) Ransomware DMA Locker's encryption may be weak, but its flaws are dangerous**
A newly discovered ransomware known as DMA Locker could potentially cause some major headaches, but not necessarily in the way its creators intended. According to cyberthreat security firm Malwarebytes in a blog post published yesterday, it is actually quite easy to undo DMA Locker's encryption, but because it's coding is so shoddy, the malware sometimes crashes before the victim ever receives a ransom demand. Consequently, users may find their computers inoperable without ever knowing that the ransomware is the culprit. The Malwarebytes analyst who authored the report, who goes by the alias Hasherzade, told SCMagazine.com, "For sure being locked out without any information is more dangerous [than the encryption itself], because users have no hint where to start searching for help." The ransom message, which has been observed in English and Polish so far, is supposed to instruct victims to pay 2 Bitcoin (the equivalent of $370 U.S.) to recover their files. Those who pay are given a 32-character decryption key to enter into a text field in order to render their files usable again. First discovered in November 2015, DMA Locker remains a small-scope operation with only one known case in the wild. Nevertheless, it reflects a growing trend, said Hasherzade. "Since ransomware is becoming more and more popular, we've noticed that the quality of the code is decreasing. This leads us to believe that even novice cybercriminals are trying their hand at developing their own ransomware," he explained. According to Malwarebytes, the ransom note -- when it actually materializes -- reads: "All of files [sic] are locked with asymetric [sic] algorithm using AES-256 and then RSA-2048 cipher. In reality, DMA Locker does not use these advanced encryption specifications, and Malwarebytes analysts have already cracked the code. According to the blog post, the encryption key is hard-coded into the malware's binary, and plainly visible to see. The malware tries in vain to hide the key by making a modified copy of itself without the key and then deleting the original. But a security analyst need only examine the malware-laced file originally opened by the victim in order to pull up the key. "We are currently analyzing the samples we have deeper, in addition to new variants of this malware," said Hasherzade, who did note that DMA Locker is gradually improving in quality with each subsequent edition. He recommended that users infected with DMA Locker seek the help of an industry professional for further guidance. (scmagazine.com, 03Feb16)

**(U) Malwarebytes still fixing flaws in antivirus software**
Malwarebytes said it could take three of four weeks to fix flaws in its consumer product that were found by a Google security researcher. The company has fixed several server-side vulnerabilities but is still testing a new version of its Anti-Malware product to fix client-side problems, CEO Marcin Kleczynski said in a blog post. In the meantime, customers can implement a workaround: those using the premium version of Anti-Malware "should enable self-protection under settings to mitigate all of the reported vulnerabilities," he wrote. Kleczynski apologized, saying vulnerabilities are a reality that come with software development. "While these things happen, they shouldn't happen to our users," he wrote. Google researcher Tavis Ormandy uncovered several issues with the Anti-Malware product, including that it doesn't use encryption when downloading fresh signatures. That opens the possibility for a man-in-the-middle attack, Ormandy said in an advisory. An attacker could potentially replace the signature file. Ormandy also found three other issues, including a privilege escalation flaw. He reported the flaws to Malwarebytes in November and gave the company 90 days to fix them before going public. (IDG News Service, 02Feb16)

**(U) Severe and unpatched eBay vulnerability allows attackers to distribute malware**
Check Point researchers have discovered a severe vulnerability in eBay's online sales platform, which allows criminals to distribute malware and run phishing campaigns. This vulnerability allows attackers to bypass eBay's code validation and control the vulnerable code remotely, to execute malicious Javascript code on targeted eBay users. If this flaw is left unpatched, eBay users will continue to be exposed to potential phishing attacks and data theft. An attacker can target eBay users by setting up an eBay store with listings for products. The listings page contains the malicious code. Customers can be tricked into opening the page using a pop-up message on the attacker's eBay store enticing the user into downloading a new eBay mobile application, by offering a one-time discount. If a user taps the download button, they unknowingly download a malicious application to their device, and the code will be executed by the user's browser or mobile app, leading to multiple ominous scenarios that range from phishing to download of malware. "The eBay attack flow provides cybercriminals with a very easy way to target users: sending a link to a very attractive product to execute the attack. The main threat is spreading malware and stealing private information. Another threat is that an attacker could have an alternate login option pop up via Gmail or Facebook and hijack the user's account," said Oded Vanunu, Security Research Group Manager at Check Point. After the flaw was discovered, Check Point disclosed details of the vulnerability to eBay on 15 Dec 2015. However, on 16 January 2016, eBay stated that they have no plans to fix the vulnerability. (net-security.org, 02Feb16)

**(U) Researchers spot bugs in toys that could expose personal data**
Researchers at Rapid7 discovered vulnerabilities in Fisher-Price's Smart Toy and hereO's GPS platforms that could allow an attacker to collect the personal information of a user. The Smart Toy is a stuffed animal that connects to an online account via WiFi to provide users with a customizable educational and entertainment experience. The toy's platform contained an improper authentication handling vulnerability that could allow an unauthorized user to obtain a child's name, age, date of birth, gender, spoken language and more, according to a 2 February security blog post. Many of the platform's web service application program interface (API) calls didn't appropriately verify the "sender" of messages and could allow a would-be attacker to send requests that shouldn't be authorized under ideal operating conditions, according to the post. In addition to compromising privacy, an attacker could use the bug to launch social engineering campaigns or to force the toy to perform actions that users didn't intend, the researchers wrote. The hereO GPS platform contained an authorization bypass vulnerability which could allow an attacker to access every family member's location, according to the post. Once exploited, an attacker could discreetly add their account to any family's network and manipulate notifications through social engineering to avoid detection. Researchers gave the example of an attacker adding themselves to a family's network under the "name" 'This is only a test, please ignore,' in an attempt to avoid raising suspicion. Both vulnerabilities were reported to their respective vendors and have since been rectified. Other IoT toys have been found to pose risks to users as well. Last year, researchers identified security concerns in Mattel's Hello Barbie that could allow an attacker to extract, internal Mac addresses, WiFi network names, account IDs, and MP3 files from the popular doll. ToyTalk, the company that operates the doll's speech services, reportedly admitted the doll could be hacked but said the vulnerable information did not identify children, nor did it compromise any audio of a child speaking. (scmagazine.com, 02Feb16)

**(U) Despite progress, DOD systems still vulnerable to hacking**
Despite some key improvements from the previous fiscal year, Defense Department missions and systems remain vulnerable to hacking, according to an annual report from the Pentagon's weapons tester. Cyber testing teams deployed on DOD networks were "frequently in a position to deliver cyber effects that could degrade the performance of operational missions," the fiscal 2015 report from the Office of the Director of Operational Test and Evaluation (DOT&E) states. The report also notes that in the past year, the Pentagon has made important strides in cyber defense, including enhanced protection of some network elements and greater awareness from leaders of the potential impact of a hack on critical missions. But DOD network operators still face a daunting task in securing their networks. The report also reveals that for months DOD personnel have been unable to access maintenance information on the F-35 stored in a Lockheed Martin database because it does not comply with information assurance policies implemented by US Cyber Command in August 2015. (fcw.com, 01Feb16)

**(U) A hacker's hidden stash may be in your HP printer's hard drive**
Security researcher Chris Vickery has discovered that HP LaserJet printers may be abused as an anonymous data storage unit by malicious actors, thanks mainly to a default setting that sets up an FTP server via port 9100. The feature in question has its place in HP's LaserJet business-grade series of laser printers. It allows a company's employees to host large troves of data on the device while it's being printed. Since these devices are usually placed on corporate networks, if sysadmins forget to protect this equipment behind a firewall, or the device has a public accessible IP, an unknown attacker could access the HP printer via port 9100 and use it as a secret storage device to host malicious files. These can be anything from malicious scripts to illegal or copyrighted material, all saved and accessed from the device with no alarms bells ringing on the printer. The only evidence left is in network logs, but very few admins scan for traffic in and out of a printer. Vickery says, the only way to protect from involuntarily being part of cyber-crime is to put the printer behind a firewall, or tweak its settings and disable the FTP storage if not used. A quick Shodan search for LaserJet and port 9100 shows around 20,000 exposed printers accessible right now. (Softpedia, 30Jan16)

*Incidents of Interest:*

**(U) AnonSec hacked NASA and tried to crash drone in the Pacific Ocean**

Hacker group AnonSec has published a data dump that contains the details of 2,414 NASA employees, along with 631 videos recorded from various NASA aircraft and weather radars, and 2,143 flight logs. In the explainer that comes along with the data dump, AnonSec says the group hacked NASA by accident in 2013, when one of the Gozi viruses they released online infected one of the agency's servers. Using this initial access, the group's hackers managed to brute-force the server's root account in 0.32 seconds due to an extremely simple admin password. The group did not only maintain access to the hacked server, but as time went by, they also managed to extend their reach inside NASA's internal network, eventually breaking into three NAS (Network Attached Storage) devices. NASA was using these devices to download and then back up flight plans from its drone missions. AnonSec members rooted these devices as well and later stole some of the data stored on the hard drives. Later on, the hackers also took over CCTV feeds from the Glenn Research Center, Goddard Space Flight Center, and Dryden Flight Research Center. AnonSec members also discovered recorded videos from regular NASA missions that involved Global Hawk drones and Operation Ice Bridge. While analyzing some network traffic, the hackers found that NASA engineers were often loading a predetermined flight plan for most of their drone missions. Employing a simple MitM (Man-in-the-Middle) attack, the hackers intercepted one of these flight plans and replaced it with one of their own, which had one of NASA's $222.7 million Global Hawk drones crashing in the middle of the Pacific Ocean. Despite managing to upload a custom .gpx file that controlled the drone according to AnonSec's desires, one of NASA's engineers detected a change in the drone's original plan and took manual control of the drone. Soon after this incident, NASA realized what happened, and AnonSec lost access to the NASA servers. A screenshot released by AnonSec shows that the drone takeover event took place on 9 April 2015. Before releasing their files via their Facebook page and InfoWars, the hackers tried to contact Wikileaks and The Guardian. After a pre-briefing and with early access to the data, InfoWars confirmed that the data dump contained accurate information on 2,414 NASA employees that included name, email, and telephone numbers. AnonSec justified their actions saying that the US and NASA have long engaged in climate engineering tactics (cloud seeding or chemtrails) that have manipulated local and global weather. (Softpedia, 02Feb16)

OGA

[redacted]

**(U) Ransomware infection cripples UK city for six days**

It took six days for Lincolnshire city officials to resume normal activities after a ransomware infection locked up City Council computers last Tuesday, 26 January 2016. Initial reports from local newspaper The Lincolnite said that the ransomware authors were requesting payment of £1 million ($1.43 million) to unlock the affected computers. The newspaper corrected its reporting four days later after city officials had a chance to investigate the issue in depth, and said that the ransomware's authors were only asking for the equivalent of $500 in Bitcoin. The ransomware locked up several computers and the adjacent data, causing outages in various local services that were using it. The Lincolnshire services that had to alter their normal operations include the Lincolnshire Fire and Rescue Department, the CallConnect rural bus service, public libraries, and social service workers who had to return to filling in forms by hand. As soon as the infection was detected, City Council officials called local police officers to help with the investigation. The IT network was also taken offline to prevent further damage, and the affected computers were isolated. This past Sunday, city officials announced that their IT system would be brought online this Monday morning. Officials did not say which ransomware strain infected Lincolnshire City Council computers, but they specifically said it was not CryptoLocker, a famous crypto-ransomware that was one of 2014's most spread ransomware families. (Softpedia, 01Feb16)

OGA

[redacted]

*Items of Interest*

**(U) NSA faces US probe over Juniper backdoor code claims**
The US government has launched an investigation following the discovery of "unauthorized code" in firewall software from Juniper Networks to determine whether it was inserted by the NSA, according to Reuters. Juniper revealed in December that it had found two pieces of code in the firm's ScreenOS software that could give remote hackers the ability to spy on secure virtual private network connections. Analysis indicated that the backdoor code was inserted as far back as 2012. The US House Committee on Oversight and Government Reform sent a number of official letters on 21 January asking various government departments to audit their networks and report on how they responded to the problem. Will Hurd, a Texas republican and formerly of the CIA, who now runs a US technology subcommittee, confirmed to Reuters that his investigation will include the possibility of NSA involvement. "How do we understand the vulnerabilities that created this problem and ensure this kind of thing doesn't happen in the future?" he asked. "I don't think the government should be requesting anything that weakens the security of anything that is used by the federal government or American businesses." A report in German publication Der Spiegel said that the NSA has used persistent malware to burrow into Juniper's firewalls and install NSA programs into the firm's computers. (v3.co.uk, 29Jan16)

**(U) US Army seeking strategy for cyber militias 'over next 3 years'**
The US Army will be looking at how to stand up cyber units outside of active duty officers in the next several years, US Army Cyber Command Commanding General Edward Cardon stated on Friday. "We are looking, with the [National] Guard and the Reserve, how do we recruit, and how do we mobilize them and how do we manage them [because] there are a lot of incidents," Cardon said of the cyber units. "It's not like you need them for a year, you normally need them for about ten days." Cardon questioned whether the United States should use the Estonian model of a "cyber militia," where hundreds of citizens are given training, and can be called to act as a cyber volunteer force. "Over the next three years, you are going to see a lot of work on this," Cardon noted. Currently, the US Army has 41 cyber units, approximately half of which are active duty, while the rest train on a rotating basis in the National Guard and Reserve Corps. The cyber unit service began in 2012 and employs approximately 6,000 personnel across all service branches. (Sputnik, 29Jan16)

[redacted] OGA

**(U) VirusTotal adds support for scanning malicious firmware images**
VirusTotal has announced initial support for detecting and then properly analyzing firmware images. The new feature should come in handy to users who suspect they might be infected with rootkit malware. In the past years, malware targeting a computer's BIOS (Basic Input/Output System) and UEFI (Unified Extensible Firmware Interface) firmware images has grown in numbers, with the most famous case coming out of the Hacking Team data breach. The reason cyber-criminals are targeting UEFI and BIOS images is because they can persist malicious code between PC reboots and even PC reinstalls. Additionally, antivirus engines can't reach that deep inside a computer's system to scan for viruses in the firmware. VirusTotal's new feature is available starting today, and you can extract your firmware code, optionally remove personally identifiable information (like WiFi passwords, hostnames, etc.), and then upload it to VirusTotal through the regular homepage form. Once the results show up, just check out the "File detail" and "Additional information" tabs. VirusTotal will automatically break down your firmware, analyze each file, and compare it to the virus databases of all the antivirus engines it supports. If something shady comes up, you'll see it in the "File detail" tab, marked with an orange or red icon. When this happens, then it may be the time to wipe your BIOS/UEFI and reinstall it from scratch. For this operation, non-technical users might need to hire an IT professional. (Softpedia, 28Jan16)

**(U) DHS $6 Billion Firewall May Not Be Effective In Keeping Hackers Out of Government, Audit Says**
A firewall run by the Department of Homeland Security meant to detect and prevent nation-state hacks against the government functions ineffectively, according to a sanitized version of a secret federal audit. EINSTEIN relies on patterns of attacks, called signatures, to spot suspicious traffic, but it does not scan for 94 percent of commonly known vulnerabilities or check web traffic for malicious content. Those are two of the many failings uncovered in a damning public version of a "for official use only" Government Accountability Office report. In addition, the prevention feature of the system is only deployed at five of the 23 major nondefense agencies. Lawmakers in November 2015 suggested the then-confidential audit of EINSTEIN, formally called the National Cybersecurity Protection System, or NCPS, would prove the hacker surveillance system is not government-wide. The newly released audit corroborates their views and points out other misaligned objectives and technologies in a $6 billion project DHS cannot say helps combat hackers, according to auditors. "Until NCPS' intended capabilities are more fully developed, DHS will be hampered in its abilities to provide effective cybersecurity-related support to federal agencies," GAO director of information security issues, Gregory C. Wilshusen, and Nabajyoti Barkakati, director of the GAO Center for Technology and Engineering, said in the audit, which was released Thursday. The auditors focused their study on the departments of Energy and Veterans Affairs, as well as the General Services Administration, the National Science Foundation and the Nuclear Regulatory Commission. EINSTEIN works by pushing out signatures of known attack patterns to 228 intrusion-detection sensors placed throughout the dot-gov network. The sensors analyze patterns in agency traffic flows to see if they match any of the signatures. "However, the signatures supporting NCPS's intrusion detection capability only identify a portion of vulnerabilities associated with common software applications," the authors reported. Of five client applications reviewed -- Adobe Acrobat, Flash, Internet Explorer, Java and Microsoft Office -- the system was able to flag, to some extent, only 6 percent of all the security bugs tested. -- 29 out of 489 vulnerabilities. One reason for the blind spots, according to the auditors, is that EINSTEIN does not sync with the standard national database of security flaws maintained by the National Institute of Standards and Technology. Homeland Security officials said they weren't required to link up the signatures with the vulnerability database when EINSTEIN was first developed. DHS "has acknowledged this deficiency" and plans to address it in the future, according to the audit. (NextGov, 28Jan16)

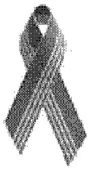
**(U) Tweeting at a Federal Agency?**
The New 'US Digital Registry' Can Tell You for Sure. A new registry of verified government social media accounts could help the public beware of online digital doppelgängers and allow developers to create tailored applications that pull in data from thousands of official government social media accounts. The US Digital Registry aims to be the authoritative source for all official social media accounts used by federal agencies. The registry also lists official government mobile apps and mobile websites. Besides authenticating government accounts, General Services Administration officials who worked on compiling the registry over the past year hope it can also help developers create new apps and widgets built on the data and content agencies produce every day across a plethora of social media accounts and other third-party sites. GSA's in-house SocialGov group announced the new public registry via third-party blog publisher Medium. "It's easy for the government to verify the official status and accountability of a website. . because you can see dot-gov and dot-mil at the end of it," Justin Herman, GSA's social media lead, told Nextgov in an interview. "When you're dealing with third-party sites, I mean most of them don't have even the little blue check mark" -- the signal used by Facebook and Twitter to denote so-called verified accounts. Herman said his team met with representatives from both Facebook and Twitter in Washington on Thursday to discuss how the companies can use the new registry during their own verification processes. GSA has also had initial conversations with researchers, data analysts and other companies about how they can use the data in the registry via application programming interfaces(APIs) to create new services built on government data shared on social media and other third-party sites. There's also a cybersecurity component to the roster, Herman added, citing the frequent phishing scams in which fraudsters try to glean information from Internet users by posing as government officials. "People can ensure the fact that when they're asking questions about their federal student loans or their veterans' health benefits, that the people that they're engaging with are the [Department of Veterans Affairs] and it is Federal Student Aid and not, let's say, a malicious body who might be interested in collecting personally identifiable information from them or to post as a government agency and get them to buy a service or pay for something that is unnecessary," Herman said. Agency social media managers are currently adding accounts and account details to the registry during what GSA is calling a "verification sprint," which is expected to wrap up by the end of the month. By then, GSA expects to see some 6,000 accounts listed in the registry. (NextGov, 28Jan16)

---

[redacted]

(b)(3) 10 USC ⊥ 424

Note: This is not original product but is consolidated from various sources.



[redacted]

(b)(3) 10 USC ⊥ 424