[redacted] Cyber-Threat Newsletter – 24 Oct 16

(b)(3) 10 USC ⊥ 424

Patches & Updates of the Week:

(U) Oracle fixes 100s of vulnerabilities that put enterprise data at risk

(U) Oracle has released another large batch of patches, fixing many critical vulnerabilities in enterprise products that are used to store and work with critical business data. About 40 percent of the patched flaws are located in Oracle E-Business Suite, Oracle Fusion Middleware, Oracle PeopleSoft, Oracle Retail Applications, Oracle JD Edwards, Oracle Supply Chain Products and Oracle Database Server. Many of these flaws can be exploited remotely without authentication to compromise the affected components. In total, Oracle's October Critical Patch Update (CPU) contains 253 security fixes across hundreds of products including database servers, networking components, operating systems, application servers and ERP systems. In databases, 31 flaws were patched in MySQL and 12 in the Oracle Database Server. Another 21 flaws were fixed in Oracle E-Business Suite, the company's main business software bundle. Fourteen of these vulnerabilities can be exploited remotely without authentication. There were 29 flaws were patched in the Oracle Fusion Middleware, which includes Oracle Big Data Discovery, Oracle Web Services, Oracle WebLogic Server, Oracle GlassFish Server, Oracle iPlanet Web Server and Oracle Outside In Technology that's used in many third party products to manipulate file formats. Nineteen of these vulnerabilities can be exploited remotely without authentication and five of them are rated critical and could lead to a complete compromise of the affected components. The Oracle PeopleSoft family of products received 11 security fixes, the Oracle JD Edwards products received 2 and Oracle Siebel CRM, three. Many flaws were also fixed in Oracle's industry-specific applications such as those for financial services, commerce, retail, insurance, hospitality and health sciences. On the OS and virtualization front, 16 vulnerabilities were fixed in Solaris and other Sun-inherited products, such as the Sun ZFS Storage Appliance. Thirteen flaws were also fixed in VirtualBox, Virtual Desktop Infrastructure and Sun Ray Operating Software. Seven vulnerabilities that can be exploited remotely without authentication have also been fixed in Java SE, three of them being rated critical. Overall, this is the second-largest CPU ever released by Oracle and touches almost all of the company's products. All of Oracle CPUs released this year -- they are released quarterly -- have exceeded 200 security fixes. This is compared to an average of 161 fixes per CPU in 2015 and 128 in 2014. (IDG News Service 19Oct16)

~~(U//FOUO)~~ Microsoft fixes 37 flaws in monthly Patch Tuesday

~~(U//FOUO~~) On 11 October, Microsoft issued patches for 37 newly disclosed security flaws, according to an online security blog. The release had five bulletins rated "critical," which addressed flaws in Edge, Graphics Component, Internet Explorer (IE), Video Control, and Adobe Flash Player; and four bulletins rated "important" that addressed flaws in Office, Windows Diagnostic Hub, Windows Kernel-Mode Drivers, and Windows Registry. One bulletin rated as "moderate" addressed a flaw in the Microsoft Internet Messaging API. The IE bulletin fixed 11 flaws and the Edge bulletin fixed 13; seven flaws affected both Edge and IE. Most were memory corruption flaws that allowed arbitrary code execution and others involved privilege escalation and information disclosure flaws. (blog.talosintel.com | 11 Oct 16)

Threats & Vulnerabilities of the Week:

(U) Securing medical devices: Cybersecurity spending to triple by 2021

(U) The medical IoT is set to transform healthcare through smart medical devices. However, their success is in jeopardy if cybersecurity concerns are not addressed immediately. ABI Research believes that the millions of connected medical devices introduce dangerous new threat vectors into the healthcare IT infrastructure, and will seriously undermine patient safety and effective care delivery if left unchecked. "We estimate spending by healthcare providers and OEMs on healthcare cybersecurity to reach $5.5 billion by 2016," says Michela Menting, Research Director at ABI Research. "However, only $390 million of that will be dedicated to securing medical devices. Healthcare stakeholders have to understand that there is a new hostile environment that will emerge around networked medical devices and that threat actors have multiple levels of skills and diverging motivations for attacking the medical IoT". The money spent on securing medical devices will primarily be due to OEMs embedding security in the hardware, reviewing, analyzing, pen testing, developing patches, and performing OTA updates, among other functions. The rest of the expenditure will focus on data protection. But medical devices suffer from numerous vulnerabilities, and many often compound several critical vulnerabilities: code errors in software, use of hardcoded passwords, disabling of firewalls, lack of authentication mechanisms, unencrypted communications, among many other issues. Protecting devices requires addressing technical issues, healthcare delivery, and business challenges. To do this, collaboration across the various stakeholder silos is necessary. The industry, however, is at the beginning stages of the discussion. Globally, the efforts are poor, and the US is the only country currently putting significant energies into the matter. However, awareness is growing, which will push spending on devices to triple globally by 2021, resulting primarily from dynamic US public and private efforts in the space. A few companies are already fully embracing medical device cybersecurity, including Battelle, Coalfire, Dräger, Extreme Networks, Sensato, Synopsys, UL, and WhiteScope. (helpnetsecurity.com 19Oct16)

(U) Poor password and username management leaves many home routers vulnerable

(U) About 15 percent of all home routers are unsecure, according to a study recently released by ESET. ESET took a look at home 12,000 routers and found that 15 percent had weak passwords with the default 'admin' being the username. "During the test, common default usernames and passwords, as well as some frequently used combinations, were tested. It's disturbing that more than one in seven of such simple simulated attacks was successful," wrote Peter Stancik, ESET researcher. The research firm also found several other problems within the routers. Just over 50 percent of the issues were bad access vulnerabilities and 40 percent of the routers had a command injection vulnerability. The latter makes the router vulnerable to remote command execution. Ten percent of the routers were found vulnerable to cross-site scripting, which if exploited would allow an attacker to modify the routers configuration to run an unauthorized script. (scmagazine.com 19Oct16)

(U) "Lurking malice" found in cloud hosting services

(U) A study of twenty major cloud hosting services has found that as many as 10 percent of the repositories hosted by them had been compromised -- with several hundred of the "buckets" actively providing malware. Such bad content could be challenging to find, however, because it can be rapidly assembled from stored components that individually may not appear to be malicious. To identify the bad content, researchers created a scanning tool that looks for features unique to the bad repositories, known as "Bars". The features included certain types of redirection schemes and "gatekeeper" elements designed to protect the malware from scanners. Researchers from the Georgia Institute of Technology, Indiana University Bloomington and the University of California Santa Barbara conducted the study. Georgia Tech says that the research, believed to be the first systematic study of cloud-based malicious activity, will be presented 24 October at the ACM Conference on Computer and Communications Security in Vienna, Austria. The work was supported in part by the National Science Foundation. "Bad actors have migrated to the cloud along with everybody else," said Raheem Beyah, a professor in Georgia Tech's School of Electrical and Computer Engineering. "The bad guys are using the cloud to deliver malware and other nefarious things while remaining undetected. The resources they use are compromised in a variety of ways, from traditional exploits to simply taking advantage of poor configurations". Beyah and graduate student Xiaojing Liao found that the bad actors could hide their activities by keeping components of their malware in separate repositories that by themselves didn't trigger traditional scanners. Only when they were needed to launch an attack were the different parts of this malware assembled. "Some exploits appear to be benign until they are assembled in a certain way," explained Beyah, who is the Motorola Foundation Professor and associate chair for strategic initiatives and innovation in the School of Electrical and Computer Engineering. "When you scan the components in a piecemeal kind of way, you only see part of the malware, and the part you see may not be malicious". In the cloud, malicious actors take advantage of how difficult it can be to scan so much storage. Operators of cloud hosting services may not have the resources to do the deep scans that may be necessary to find the Bars -- and their monitoring of repositories may be limited by service-level agreements. (homelandsecuritynewswire.com 19Oct16)

(U) Beware the Internet of Unpatchable Things: Akamai

(U) A recent spate of attacks involving attackers using IoT devices to remotely generate attack traffic by using a 12-year old vulnerability in OpenSSH have been discovered by researchers at Akamai Technologies. Akamai notes that the research and subsequent advisory do not introduce a new type of vulnerability or attack technique, but rather a continued weakness in many default configurations of Internet-connected devices. These devices are now actively being exploited in mass-scale attack campaigns against Akamai customers. The Threat Research Team said it has observed incidents of what it has called SSHowDowN Proxy attacks originating from the following types of devices: CCTV, NVR, DVR devices (video surveillance) Satellite antenna equipment Networking devices (e.g. Routers, Hotspots, WiMAX, Cable and ADSL modems, etc.) Internet connected NAS devices (Network Attached Storage) Compromised devices are being used for mounting attacks against a multitude of internet targets and internet-facing services, such as HTTP, SMTP and Network Scanning. It is also being used to launch attacks against internal networks that host these connected devices. Once malicious users access the web administration console, they have been able to compromise the device's data and, in some cases, fully take over the machine. "We're entering a very interesting time when it comes to DDoS and other web attacks; 'The Internet of Unpatchable Things' so to speak," explained Ory Segal, senior director for threat research at Akamai. "New devices are being shipped from the factory not only with this vulnerability exposed, but also without any effective way to fix it. We've been hearing for years that it was theoretically possible for IoT devices to attack. That, unfortunately, has now become the reality". (Telecom Asia 19Oct16)

(U) Government IT pros say smart cities have no cybersecurity

(U) Tripwire research indicates smart grids and transportation among the services most exposed to cyberattack risks. Ninety-eight percent of government IT professionals see smart cities as not having any protection from cyberattacks and 55 percent blame the cities for not focusing on cybersecurity resources, according to a survey by cybersecurity solutions provider Tripwire. Smart grids, one of the smart city services, were seen by 38 percent to be more exposed to cyber risks than others, while 26 percent considered transportation to be more vulnerable. Other services include surveillance cameras, wastewater treatment, etc. "Smart city initiatives are pushing the technological envelope for urban infrastructure management, and it's clear from the survey results that cybersecurity is being left out of the conversation," says Tim Erlin of Tripwire. The reason for this, believe 61 percent, could be budgets, while 60 percent say it is political interference. Read the full survey on the Tripwire website. (Dark Reading 19Oct16)

(U) Hackers create more IoT botnets with Mirai source code

(U) Malware that can build botnets out of IoT products has gone on to infect twice as many devices after its source code was publicly released. The total number of IoT devices infected with the Mirai malware has reached 493,000, up from 213,000 bots before the source code was disclosed around 1 October, according to internet backbone provider Level 3 Communications. "The true number of actual bots may be higher," Level 3 said in a Tuesday blog post. Hackers have been taking advantage of the Mirai malware's source code, following its role in launching a massive DDOS (distributed denial-of-service) attack that took down the website of cybersecurity reporter Brian Krebs. Unlike other botnets that rely on PCs, however, Mirai works by infecting internet-connected devices such as cameras and DVRs that come with weak default usernames and passwords. Since Mirai's source code was released, hackers have been developing new variants of the malware, according to Level 3. It has identified four additional command-and-control servers associated with Mirai activity coming online this month. About half of the infected bots Level 3 has observed resided in either the US or Brazil. More than 80 percent of them were DVR devices. "We have observed several attacks using more than 100 Gbps" of traffic, Level 3 said. "Large armies of bots participated in attacks, with several using over 100,000 bots against the same victim". A few vendors that produce devices vulnerable to Mirai are encouraging their customers to take steps to mitigate the risk. Sierra Wireless, for instance, has issued a bulletin, advising users to reboot one of their products and change the default password. However, it's unclear if other vendors are taking any steps to do the same. (IDG News Service 18Oct16)

(U) Critical flaws found in open-source encryption software VeraCrypt

(U) A new security audit has found critical vulnerabilities in VeraCrypt, an open-source, full-disk encryption program that's the direct successor of the widely popular, but now defunct, TrueCrypt. Users are encouraged to upgrade to VeraCrypt 1.19, which was released Monday and includes patches for most of the flaws. Some issues remain unpatched because fixing them requires complex changes to the code and in some cases would break backward compatibility with TrueCrypt. However, the impact of most of those issues can be avoided by following the safe practices mentioned in the VeraCrypt user documentation when setting up encrypted containers and using the software. While VeraCrypt is available for multiple operating systems, it is on Windows where it has the biggest impact, because there aren't many free full-disk encryption options on Windows that also allow encrypting the OS drive. Microsoft's BitLocker disk encryption technology is only included in the professional and enterprise versions of Windows and most other solutions are commercial. This is what made TrueCrypt so popular in the first place and why its sudden demise left a big void. (IDG News Service 18Oct16)

(U) Locky ransomware accounted for 97 percent of all malicious email attachments

(U) If you've received spam emails bearing a file attachment in the last three months, it's very likely that the file contains a version of the Locky ransomware, according to Proofpoint's Quarterly Threat Summary for Q3 2016. A previous report from Cisco said that spam numbers returned to record levels seen last time in the early 2010s. That report included all spam categories, such as pharma, dating, and pump-and-dump campaigns. According to Proofpoint, the number of spam emails spreading malware-laced files reached all-time high numbers in Q3 2016. King among all malware families that leveraged spam campaigns to spread was the Locky ransomware, found in 96.8 percent of all malicious spam file attachments. In a vast majority of cases, this manifested as a ZIP file containing a JavaScript file inside, but crooks also leveraged Offices documents that contained malicious macro scripts, HTA (HTML executable) files, and WSF (Windows Script) files. The rest of the Top 5 most spammed malware includes the Pony infostealer, the Vawtrack banking trojan, the Tordal (Hancitor) malware dropper, and the Panda Banker banking trojan. Besides Locky, other ransomware variants spread via spam campaigns in larger numbers included CryptFile2, MarsJoke, and Cerber. The same Proofpoint quarterly report also highlights a continuous evolution of banking trojans, who, even if were spread in far fewer numbers than in 2015, continued to be a constant threat thanks to a series of anti-detection features they added in order to avoid security software. The good news from Q3 2016 is that exploit kit activity has gone down 65 percent compared to Q2 and 93 percent relative to the start of 2016. This downfall can be attributed to the shutdown of the Angler and Nuclear exploit kits this past spring, but also to the Neutrino exploit kit entering a so-called "private mode". (Softpedia 16Oct16)

(U) Almost 6,000 online stores currently infected with card-data-stealing malware

(U) In spite of the fact that WordPress continues to be the most hacked CMS platform, compromising online shopping platforms such as Magento, OpenCart, and others is by far more lucrative for online crooks. According to Willem de Groot, security analyst for Byte.nl, the number of online shops infected with malware has skyrocketed in the past year, as crooks found that online skimming presents a greater target and more anonymity than real-world ATM skimming. The recent surge in online skimming has fueled a growth in carding sites, which now often sell payment card data stolen via compromised online store payment pages and PoS malware, rather than data acquired from ATM skimmers. De Groot, who is also one of the people behind MageReport.com, a Magento site security scanner, has been keeping track of online stores infected with malware ever since November 2015, when he first saw an uptick in such cases. A general Internet scan of 255,000 online stores has revealed the presence of various malware variants on 3,501 shops. When he repeated the scan in March 2016, he found 4,476 infected stores, which represented an increase of 28 percent. Ten months later, in September 2016, de Groot found 5,925 infected sites, up 69 percent from November 2015. With the recent discovery of the MageCart malware, de Groot repeated his scan once again, on 10 October, when he found 5,911 infected stores. The good news is that the MageCart report scared enough webmasters, and on 12 October, the number had gone down to 5,761, with 334 admins cleaning up their stores, while 170 new stores were infected. You might be tempted to think that only old and niche websites suffer such infections. It's not true. De Groot highlights some pretty high-profile sites on his most recent infection lists. He mentions the online store of Icelandic singer Bjork, the store of Audi South Africa, and the website of the NRSC (National Republican Senatorial Committee). Cleaning up these stores is not a simple job, since updating some online platforms such as Magento requires some level of technical skills, and it's not a one-click button job. But de Groot doesn't have a problem with the technical side of updating online stores, since all online platforms provide very good documentation to get this done. His problem is with the human factor, as many ignore his warning. And if the ignorance of online store owners weren't enough, de Groot, who's been keeping track of different malware families, says he's seen a rise in sophistication for the malware's code. Nowadays, malware has support for various types of checkout and payment extensions and uses very complex code obfuscation. Besides getting harder to detect, the number of online skimming malware has gone through the roof as well. De Groot says that in almost a year, online skimming malware has gone from one single threat to nine varieties and three distinct malware families. "Companies such as Visa or Mastercard could revoke the payment license of sloppy merchants," de Groot proposes. "But it would be way more efficient if Google would add the compromised sites to its Chrome Safe Browsing blacklist. Visitors would be greeted with a fat red warning screen and induce the store owner to quickly resolve the situation". De Groot says that he's been sending the Safe Browsing team reports about his findings, but currently only a handful of these sites are blacklisted. (Softpedia 14Oct16)

Incidents of Interest:

[redacted]

OGA

(U) Czech police arrest Russian hacker for cyber-attacks against the US

(U) Following a collaboration with the US Federal Bureau of Investigation (FBI), Czech national police announced yesterday the arrested of a man on suspicion of hacking various entities in the US. The suspect, who's name hasn't been released yet, was arrested in Prague, the Czech Republic's capital. The man is a Russian national, who's been living in the country with his girlfriend. Police arrested the suspect after Interpol issued a warrant for his arrest. Czech police apprehended the individual 12 hours after receiving the order. The suspect was surprised by authorities and didn't put up any resistance during the arrest. Moments after police took him into custody, the hacker fainted and lost consciousness. Police officers provided first aid, and the Russia national was later taken to a hospital. He remained in police custody. FBI officials have requested for the man's extradition to the US, where he'll have to face charges for his hacking-related crimes. The Municipal Court in Prague will decide on the extradition. Neither the Czech police or the FBI have issued any details on the charges that led to the suspects arrest. (Softpedia 19Oct16)

[redacted] OGA

(U) Shadow Brokers cancel auction of supposed NSA hacking tools

(U) The Shadow Brokers announced yesterday they plan to cancel the auction for the supposed NSA hacking tools and converting the process into a crowdfunded sale. So instead of an auction that would have awarded the highest bidder access to all the hacking tools, the group is now offering the password to everyone who contributes to an end goal of 10,000 bitcoin ($6.3 million). This change of heart comes just two weeks after the group complained about how nobody was bidding on their auction. (Softpedia 16Oct16)

[redacted] OGA

Items of Interest

(U) NirSoft's EncryptedRegView decrypts and displays secret Registry data

(U) NirSoft has released EncryptedRegView, a free tool which finds, decrypts and displays Registry data protected by Windows' DPAPI encryption scheme. DPAPI isn't widely used, even by Microsoft products, but the program managed to find Outlook passwords, Microsoft Edge details and a few other interesting items on a test PC. The program is straightforward to use. Run it as an administrator if possible, click OK on the opening dialog and watch as EncryptedRegView scans your Registry. The program displays every DPAPI-protected item it finds, with columns for Registry path, original and decrypted values, hash and encryption values, and more. Most of these items won't mean anything to the average user. You'll see a path like "HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{60782261-81D18-4323-9C64-10DE93176363}", with a cryptic hex dump, and nothing else at all. Other items could be more interesting. Our test system had several value names of "POP3 Password" with actual email passwords as the "Decrypted Value". Each of these had a Registry path including "Microsoft\Office\16.0\Outlook\Profiles", so we could see they were Outlook passwords. This could well be useful, but the program doesn't directly tell you which password belongs to which Outlook account. You would have to explore the profile path in the Registry to understand that. You can also run an advanced search at any time (Options > Advanced Search) to scan Registry files on an external hard drive, perhaps from some other PC. Note that you'll only be able to see user-encrypted data if you have that user's logon password. Overall, EncryptedRegView won't appeal to the average user, but if you're interested in computer forensics it could give you some handy clues about your target system. EncryptedRegView is a free tool for Windows XP and later. (BetaNews 19Oct16)

[redacted]

OGA

(U) Internet routing security effort gains momentum

(U) More than 40 network operators agree to filter routing information, prevent IP address-spoofing, and to work together to thwart Internet traffic abuse and problems. Cybercriminals and nation-state hackers routinely hide behind phony IP addresses to mask their location and identity, but an Internet initiative that seeks to thwart that and other malicious and inadvertent traffic on the global Net now has on board some 42 network operators crisscrossing 21 nations. The Internet Society's Mutually Agreed Norms for Routing Security (MANRS), which launched nearly two years ago as a plan for advancing the security and resilience of the Net's routing infrastructure, has signed up network operators in Asia, North and South America, Africa, and Europe, including six network providers from Russia, five in the Netherlands, five in the US, and four in Germany. AT&T, Comcast, and Level 3, are among the largest US ISPs that have joined the effort. MANRS consists of four practices: filtering, anti-spoofing, coordination among providers, and global validation. Participating network providers must deploy at least one of them (and it can't just be the coordination activity). According to the Internet Society, the majority of providers have deployed all four practices and none so far have enacted less than three of them. The effort is one element of the overall vision of updating the aging Internet architecture to address the security issues that weren't an issue back when the Net was built. Andrei Robachevsky, technology programme manager for the Internet Society, says the challenge with routing on the Net today is that each network operator must implicitly trust the routing information provided by its neighboring provider when moving traffic. MANRS basically defines a specific set of minimum measures to provider routing security across the Net, he says. Filtering helps prevent phony or incorrect routing information. Preventing traffic with spoofed IP addresses can help thwart distributed denial-of-service (DDoS) attacks, which often hide behind phony IPs. "A huge class of volumetric reflection amplification DDoS attacks' root cause is the ability to spoof traffic and IP addresses," he says. "If you close this ... it will significantly diminish the prevalence of those attacks". The other two measures are about network operators working more closely together: one is to communicate and coordinate among their peer networks to stop security threats, for example. It will help network operators know who to contact in the event of a network incident, and to keep their information updated. The other such practice is validating routing information, so now there will be a database of that information that can be used for reference, he says. Not all network operators will participate or cooperate, of course. Network operators or regions that abuse the Internet infrastructure for cybercrime or other nefarious activity won't join MANRS, according to Robachevsky, but their lack of participation ultimately could make them more conspicuous. (Dark Reading 13Oct16)

(U) One of Air Force's most important unclassified systems is now in the Oracle cloud

(U) MyPers, the Air Force's personnel portal for 1.7 million active duty and retired airmen, civilian and reservists, began operating in July out of an Oracle-managed off-premise cloud specifically designed and secured to handle some of the Defense Department's most sensitive unclassified workloads. It's the first software-as-a-service accredited implementation for a cloud provider at DOD impact level 4, according to Bill Marion, the Air Force's deputy chief information officer. More importantly, it's improving the reliability and security of one of the Air Force's most-used applications. The portal is used for transactions and questions around retirement, benefits and other personnel issues, and touches the Air Force's back-end civilian systems. MyPers' cloud instantiation achieved initial operating capability in nine months, Marion said, despite the bureaucratic challenges that come with being an early adopter of technology the Pentagon embraces cautiously. Much of that time was spent "working through security issues" inherent in migrating an outdated yet complex system to the cloud, Marion said. So far, the Oracle-managed cloud has only had of two minor outages caused by the government, not the cloud provider, according to Marion. In addition, the move caught MyPers up to present-day security and policy automation. Much of the buzz about cloud computing centers around cost savings in government, but in this case, cost savings are less important than mission performance. The more apt way to describe the Air Force's expectations for savings are in cost avoidance rather than cost savings. Efforts like the Air Force cloud transition are not yet common, but early successes could shine a light for other military branches and DOD wings looking to get off legacy systems. (NextGov, 12Oct16)

[redacted]

(b)(3) 10 USC ⊥ 424

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

[redacted]

(b)(3) 10 USC ⊥ 424