BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 11. 2017 – 21. 11. 2017

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Score
1	Oracle Releases Security Alert	Kritická	**10.0**
2	Cisco Releases Security Update	Kritická	**9.8**
3	Mozilla Releases Security Updates	Vysoká	**7.5**
4	Windows ASLR (Address Space Layout Randomization) Vulnerability	Vysoká	**7.5**
5	Multiple VMware Products vulnerabilities	Vysoká	**7.0**
6	Adobe Releases Security Updates	Vysoká	**6.8**
7	HIDDEN COBRA – North Korean Trojan: Volgmer	Vysoká	-

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
06282/2017/SKB/OBPr-024

BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 11. 2017 – 21. 11. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 10.0**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Oracle Releases Security Alert

Popis

Spoločnosť Oracle vydala bezpečnostné varovanie ohľadne zraniteľnosti základného komponentu Oracle Fusion Middleware v rámci aplikačného servera Oracle Tuxedo. Jednoducho zneužiteľná zraniteľnosť umožňuje neautorizovanému útočníkovi so sieťovým prístupom k Jolt serveru kompromitovať Oracle Tuxedo, spôsobiť čiastočné zneprístupnenie služieb Oracle Tuxedo a získať neoprávnený prístup a možnosť modifikovať kritické údaje systému alebo všetky údaje prístupné v rámci aplikačného servera.

Dátum prvého zverejnenia varovania

16. 11. 2017

CVE

CVE-2017-10266, CVE-2017-10267, CVE-2017-10269, CVE-2017-10272, CVE-2017-10278

Zasiahnuté systémy

Aplikačný server Oracle Tuxedo (verzie 11.1.1, 12.1.1, 12.1.3, 12.2.2)

Následky

Neoprávnený prístup k informáciám, Čiastočná neprístupnosť služby

Odporúčania

Spoločnosť Oracle vydala aktualizáciu uvedeného produktu, ktorá rieši predmetnú zraniteľnosť. Používateľom a administrátorom odporúčame bezodkladne daný produkt aktualizovať.

Zdroje

http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10269-4021872.html
https://nvd.nist.gov/vuln/detail/CVE-2017-10269

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Cisco Releases Security Update

Popis

Kritická zraniteľnosť aktualizačného mechanizmu produktov bežiacich na platforme Cisco Voice Operating System by mohla umožniť vzdialenému útočníkovi získať neautorizovaný prístup k dotknutým systémom a následne zvýšiť svoje prístupové práva. Zraniteľnosť sa prejavuje pri aktualizácii prostredníctvom metódy RU (Refresh Upgrade) alebo migrácii prostredníctvom metódy PCD (Prime Collaboration Deployment). Po úspešnom dokončení uvedených metód na zariadeniach zostáva zapnutý príznak továrenského režimu, v ktorom je možné vykonávať príkazy s oprávneniami používateľa root.

Dátum prvého zverejnenia varovania

15. 11. 2017

CVE

CVE-2017-12337

Vendor ID (Cisco Bug ID)

CSCvg22923, CSCvg55112, CSCvg55128, CSCvg55145, CSCvg58619, CSCvg64453, CSCvg64456, CSCvg64464, CSCvg64475, CSCvg68797

Zasiahnuté systémy

Cisco Unified Communications Manager (UCM), Cisco Unified Communication Manager Session Management Edition (SME), Cisco Emergency Responder, Cisco Unity Connection, Cisco Unified Communications Manager IM and Presence Service, Cisco Prime License Manager, Cisco Hosted Collaboration Mediation Fulfillment, Cisco Unified Contact Center Express (UCCx), Cisco SocialMiner, Cisco Unified Intelligence Center (UIC), Cisco Finesse, Cisco MediaSense.

Následky

Neoprávnený prístup k zariadeniu

Odporúčania

Spoločnosť Cisco vydala aktualizácie dotknutých produktov, ktoré riešia predmetnú zraniteľnosť. Používateľom a administrátorom odporúčame bezodkladne vykonať dané produkty aktualizovať.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-vos
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-12337

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Mozilla Releases Security Updates

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré riešia viacero zraniteľností v produktoch Firefox 57 (Quantum) a Firefox ESR 52.5. Zneužitím týchto zraniteľností by útočník mohol neoprávnene získať kontrolu and zasiahnutým systémom.

Dátum prvého zverejnenia varovania

14. 11. 2017

CVE

CVE-2017-7828, CVE-2017-7830, CVE-2017-7831, CVE-2017-7832, CVE-2017-7833, CVE-2017-7834, CVE-2017-7835, CVE-2017-7836, CVE-2017-7837, CVE-2017-7838, CVE-2017-7839, CVE-2017-7840, CVE-2017-7842, CVE-2017-7827, CVE-2017-7826

Zasiahnuté systémy

Mozilla Firefox 57 (Quantum), Firefox ESR 52.5

Následky

Neoprávnený prístup k informáciám, Neoprávnené vykonanie kódu

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov a následne ich udržiavať aktualizované.

Zdroje

https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2017/av17-170-en.aspx
https://www.mozilla.org/en-US/security/advisories/

Dôležitosť	☐ Nízka	☐ Stredná	☒ Vysoká	☐ Kritická	CVSS skóre: 7.5
Klasifikácia	☒ TLP (WHITE)	☐ Vyhradené	☐ Dôverné	☐ Tajné	
Kód sektora (dopad)					

Identifikátor

Windows ASLR (Address Space Layout Randomization) Vulnerability

Popis

Zraniteľnosť spočíva v nesprávnej aktivácii ASLR prostriedkami Microsoft EMET a Windows Defender Exploit Guard, ktorá útočníkovi umožní vykonať útočnú metódu ROP (Return Orinted Programming) a útoky založené na znovu-využití kódu.

Dátum prvého zverejnenia varovania

17.11.2017 (Posledná aktualizácia 19.11.2017)

Zasiahnuté systémy

Windows 8, Windows 8.1 a Windows 10

Vektor útoku

Funkcia ASLR načítava spustiteľné moduly na náhodné adresy v pamäti, čím poskytuje ochranu voči útočnej technike ROP (Return Oriented Programming), využívajúcej časti kódu načítavané na predikovateľné adresy. Využitie ASLR vyžaduje linkovanie kódu s príznakom /DYNAMICBASE. Zraniteľnosť spočíva v skutočnosti, že pre náhodné prideľovanie adries je potrebné mať súčasne aktivované funkcie bottom-up ASLR aj mandatory ASLR.
Prostriedky Microsoft EMET a Windows Defender Exploit Guard však aktivujú systémové ASLR bez súčasnej aktivácie ASLR, čo spôsobí načítavanie programov bez príznaku /DYNAMICBASE vždy na rovnakú adresu, po reštarte aj v rámci rôznych systémov.

Následky

Neoprávnené získanie kontroly nad zariadením, Neoprávnené vykonanie kódu

Odporúčania

Administrátorom odporúčame zaktivovať celosystémové bottom-up ASLR na systémoch s povinným ASLR. V rámci operačného systému Windows 8 a vyšších verzií možno aktiváciu vykonať prostredníctvom pridania nasledujúcej hodnoty do registrov:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel]
"MitigationOptions"=hex:00,01,01,00,00,00,00,00,00,00,00,00,00,00,00,00

Pridanie uvedenej hodnoty do registra prepíše existujúce systémové nastavenia. Prvá sekvencia 01 mení nastavenie povinného ASLR a druhá sekvencia 01 nastavenie bottom-up ASLR.

Zdroje

http://www.kb.cert.org/vuls/id/817544
https://insights.sei.cmu.edu/cert/2012/06/amd-video-drivers-prevent-the-use-of-the-most-secure-setting-for-microsofts-exploit-mitigation-exper.html
https://blogs.technet.microsoft.com/srd/2010/12/08/on-the-effectiveness-of-dep-and-aslr/
https://msdn.microsoft.com/en-us/library/bb384887.aspx

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Multiple VMware Products vulnerabilities

Popis

VMware Workstation a Fusion obsahujú zraniteľnosť založenú na pretečení zásobníka heap-u v zariadení VMNAT. Zraniteľnosť by útočník mohol zneužiť na neoprávnené spustenie kódu.

VMware Workstation a Horizon View Client pre Windows obsahujú zraniteľnosť umožňujúcu out-of-bounds zápis v rámci JPEG2000 parsera v dynamickej knižnici TPView.dll. Zraniteľnosť by útočník mohol zneužiť na neoprávnené spustenie kódu a zneprístupnenie služieb operačného systému Windows. Zraniteľnosť možno zneužiť len v prípade, že je aktivovaná funkcia visual printing.

Dátum prvého zverejnenia varovania

17. 11. 2017 (posledná aktualizácia 18.11.2017)

CVE

CVE-2017-4934, CVE-2017-4935

Zasiahnuté systémy

VMware Workstation (verzia 12.x pred 12.5.8), Fusion (verzia 8.x pred 8.5.9), Horizon View Client pre Windows (verzia 4.x pred 4.6.1)

Následky

Neoprávnené spustenie kódu, Neprístupnosť služby

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov a následne ich udržiavať aktualizované.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2017-0018.html
http://www.securityfocus.com/bid/101903
http://www.securityfocus.com/bid/101902

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Adobe Releases Security Updates

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré riešia kritické zraniteľnosti v produktoch Flash Player, Photoshop CC, Connect, DNG Converter, InDesign, Digital Editions, Shockwave Player a Experience Manager. Zneužitím niektorých zraniteľností by útočník mohol neoprávnene získať kontrolu nad zasiahnutým systémom.

Dátum prvého zverejnenia varovania

14.11.2017

CVE

CVE-2017-3112, CVE-2017-3114, CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-11303, CVE-2017-11304, CVE-2017-11291, CVE-2017-11287, CVE-2017-11288, CVE-2017-11289, CVE-2017-11290, CVE-2017-11295, CVE-2017-11302, CVE-2017-11273, CVE-2017-11297, CVE-2017-11298, CVE-2017-11299, CVE-2017-11300, CVE-2017-11301, CVE-2017-11294, CVE-2017-3109, CVE-2017-3111, CVE-2017-11296

Zasiahnuté systémy

Adobe Flash Player (27.0.0.183 a skoršie verzie), Adobe Photoshop CC 2017 (18.1.1 a skoršie v.), Adobe Connect (9.6.2 a skoršie v.), Adobe DNG Converter (9.12.1 a skoršie v.), Adobe InDesign (12.1.0 a skoršie v.), Adobe Digital Editions (4.5.6 a skoršie v.), Adobe Shockwave Player (12.2.9.199 a skoršie v.), Adobe Experience Manager (v. 6.0 až 6.3)

Následky

Neoprávnený prístup k informáciám, Neoprávnené vykonanie kódu

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov spoločnosti Adobe na najnovšiu verziu a udržiavať ich aktualizované.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb17-33.html
https://helpx.adobe.com/security/products/photoshop/apsb17-34.html
https://helpx.adobe.com/security/products/connect/apsb17-35.html
https://helpx.adobe.com/security/products/dng-converter/apsb17-37.html
https://helpx.adobe.com/security/products/indesign/apsb17-38.html
https://helpx.adobe.com/security/products/Digital-Editions/apsb17-39.html
https://helpx.adobe.com/security/products/shockwave/apsb17-40.html
https://helpx.adobe.com/security/products/experience-manager/apsb17-41.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: -**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

HIDDEN COBRA – North Korean Trojan: Volgmer

Popis

FBI (Federal Bureau of Investigation) a DHS (Department of Homeland Security) vydala tzv. spojené technické upozornenie (joint Technical Alert), ktoré obsahuje IOC (Indicators of Compromise), IP adresy systémov infikovaných malwarom VOLGMER, popis malwaru, priradené signatúry, odporúčané postupy reakcie a informácie o reportovaní incidentov.

VOLGMER je forma backdoor trójskeho koňa umožňujúceho skrytý prístup ku kompromitovaným systémom vo vládnom a finančnom sektore, automobilovom a mediálnom priemysle. Predpokladaným primárnym mechanizmom šírenia infekcie je phishing, analýza však nevylučuje použitie špeciálnych nástrojov používaných na počiatočnú kompromitáciu systémov. Z tohto dôvodu nemožno vylúčiť prítomnosť HIDDEN COBRA malwaru na prvkoch sieťovej infraštruktúry.

Zasiahnuté systémy

Sieťové systémy

IOC (Indicators of Compromise)

Kompletný list IOC nájdete na tomto odkaze:
https://www.us-cert.gov/sites/default/files/publications/TA%20VOLGMER%20IOCs.csv

MAR (Malware analysis report)

Kompletný MAR nájdete na tomto odkaze:
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF

Technická analýza

VOLGMER je backdoor trojan, ktorý používa HIDDEN COBRA, schopný pasívneho zberu informácií, aktualizácie registrov systémových služieb, downloadu a uploadu súborov, vykonávania spustiteľných kódov a pokročilého skenovania adresárovej štruktúry. Jedna z analyzovaných vzoriek obsahovala funkcie potrebné na konštrukciu a riadenie botnetu.

VOLGMER payloady nadobúdajú formu 32-bitovej aplikácií alebo dynamických knižníc (.dll). Spätnú signalizáciu na riadiaci server realizuje prostredníctvom vlastného binárneho protokolu, cez TCP porty 8080 a 8088. v niektorých prípadoch dochádza k maskovaniu komunikácie použitím SSL (Secure Socket Layer).

Kontinuálnu činnosť na zasiahnutých systémoch malware zabezpečuje svojou inštaláciou vo forme malware-as-a-service. VOLGMER následne systematicky prechádza systémové zdroje a náhodne vyberá službu, do ktorej inštaluje svoju kópiu, prepíše záznam ServiceDLL v príslušných registroch. V niektorých prípadoch vytvoreným službám priraďuje pseudonáhodné názvy pozostávajúce z pevne daných slov.

Sieťové signatúry
alert tcp any any -> any any (msg:"Malformed_UA"; content:"User-Agent: Mozillar/"; depth:500; sid:99999999;)

HBR (Host-Based Rules)
Kompletný výpis HBR (v tomto prípade YARA) pravidiel nájdete na tomto odkaze: https://www.us-cert.gov/ncas/alerts/TA17-318B

Následky
Dočasná alebo trvalá strata citlivých alebo chránených informácií, Zneprístupnenie služby, Finančné straty spojené s obnovou systémov a poškodenie dobrého mena.

Detekcia
DHS a FBI odporúčajú administrátorom siete, aby sa oboznámili s poskytnutými informáciami, vykonali analýzu, či niektorá z poskytnutých IP adries nespadá do nimi spravovaného adresného priestoru a v prípade pozitívneho nálezu podnikli kroky potrebné na odstránenie malwaru.

Odporúčania
Používateľom a administrátorom sa odporúča dodržiavať best-practice postupy na ochranu počítačových sietí: 1. Aktualizácia aplikácií a operačných systémov - Väčšina útočníkov sa zameriava na zraniteľné aplikácie a operačné systémy. Skutočnosť, že aplikácie a operačné systémy sú vždy aktualizované najnovšími aktualizáciami, výrazne znižuje možnosť využiť zraniteľnosti týchto systémov. Používajte osvedčené postupy pri aktualizácii softvéru pomocou oficiálnych aktualizácií iba z overených lokalít od dodávateľov. 2. Používanie „whitelistov“ – Whitelist v rovine určenia povolení pri spúšťaní programov a služieb je jednou z najlepších stratégií zabezpečenia, pretože umožňuje spustiť iba špecifikované programy, pričom zablokuje všetky ostatné vrátane škodlivého softvéru. 3. Udržujte antivírovú databázu vždy aktualizovanú a pred spustením aplikácií stiahnutých z Internetu vykonajte ich sken. 4. Ako dočasné riešenie odporúčame vypnúť funkciu visual printing 5. Zamedzte spúšťaniu makier z e-mailových príloh. 6. Neklikajte na neoverené webové linky v e-mailoch.

Zdroje
https://www.us-cert.gov/ncas/alerts/TA17-318B