BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 11. 2017 – 14. 11. 2017

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-023

BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 11. 2017 – 14. 11. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

#AVGater: Getting Local Admin by Abusing the Anti-Virus Quarantine

Popis

Zraniteľnosť ovplyvňuje činnosť viacerých antivírových programov prostredí Windows. Zneužitím adresárových uzlov NTFS (príkaz „mklink“) možno ovplyvniť proces obnovenia súborov umiestnených do karantény spôsobom umožňujúcim ich zápis na ľubovoľné miesto v systéme.

Dátum prvého zverejnenia varovania

10.11.2017

Vektor útoku

Antivírový program lokalizuje škodlivý súbor a umiestni ho do karantény. Zneužitím adresárových uzlov NTFS prostredníctvom príkazu „mklink“ dochádza k presmerovaniu pôvodného súboru na iné miesto, napr. do priečinka v rámci C:\Program Files alebo C:\Windows. Počas obnovenia súboru dochádza k zneužitiu systémových oprávnení služby antivírového programu, ktorý umožní zápis súboru do priečinka, do ktorého za normálnych okolností prihlásený používateľ nemá právo zapisovať. Následne na základe princípu činnosti vyhľadávania DLL knižníc dochádza k načítaniu škodlivého súboru iným procesom operačného systému Windows a vykonaniu škodlivého kódu v rámci DDLMain. Uvedeným postupom útočník môže získať plnú kontrolu nad zariadením.

Zasiahnuté systémy

Windows, Kaspersky, ZoneAlarm, IKARUS security software, Malwarebytes

Následky

Neoprávnené vykonanie kódu, Neoprávnené získanie kontroly nad zariadením

Odporúčania

Odporúčame bezodkladnú aktualizáciu dotknutých antivírových programov na najnovšiu verziu a bežným používateľom zakázať možnosť obnovenia súborov umiestnených do karantény.

Zdroje

https://bogner.sh/2017/11/avgater-getting-local-admin-by-abusing-the-anti-virus-quarantine/
https://www.bleepingcomputer.com/news/security/antivirus-engine-design-flaw-helps-malware-sink-its-teeth-into-your-system/
https://arstechnica.com/information-technology/2017/11/how-av-can-open-you-to-attacks-that-otherwise-wouldnt-be-possible/

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

Identifikátor

Joomla! Releases Security Update

Popis

Spoločnosť Joomla! vydala aktualizáciu svojho redakčného systému na verziu 3.8.2, ktorá rieši 3 zraniteľnosti, ktoré by vzdialený útočník mohol zneužiť na získanie prístupu do systému a k informáciám s citlivým obsahom:
1. Nesprávne zakončovanie reťazcov a overovanie vstupných hodnôt v autentizačnom plugin-e LDAP môže viesť k odhaleniu používateľského mena a hesla.
2. Bug umožňujúci útočníkom obídenie dvojfaktorovej autentifikácie používateľa.
2. Logická chyba v com_fields umožňuje neautorizovaným používateľom získať informácie ohľadne špecifických nastavení systému.

Dátum prvého zverejnenia varovania

07. 11. 2017

CVE

CVE-2017-14596, CVE-2017-16634, CVE-2017-16633

Zasiahnuté systémy

Joomla! verzie 1.5.0 až 3.8.1, Joomla! verzie 3.2.0 až 3.8.1, Joomla! verzie 3.7.0 až 3.8.1

Následky

Neoprávnený prístup k informáciám, Neoprávnený prístup do systému

Odporúčania

Spoločnosť Joomla! vydala aktualizáciu 3.8.2, ktorá rieši uvedené zraniteľnosti, preto odporúčame bezodkladne vykonať aktualizáciu redakčného systému.

Zdroje

https://www.joomla.org/announcements/release-news/5716-joomla-3-8-2-release.html
https://blog.ripstech.com/2017/joomla-takeover-in-20-seconds-with-ldap-injection-cve-2017-14596/
https://www.securitytracker.com/id/1039757

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

Identifikátor

Ubuntu Security Notice USN-3478-1: Perl vulnerabilities

Popis

Zraniteľnosti využívajú chybu parsera pri vyhodnocovaní regulárnych výrazov špecifického tvaru. Útočník následne môže spôsobiť pád Perl-u, vedúci k neprístupnosti poskytovaných služieb alebo k vykonaniu ľubovoľného kódu.
Prvá zraniteľnosť využíva pretečenie zásobníka heap-u vo funkcii S_regatom v rámci regcomp.c, ktoré možno využiť na zneprístupnenie služby použitím regulárneho výrazu zakončeného s '\N{}'.
Druhá zraniteľnosť využíva pretečenie zásobníka vo funkcii S_grok_bslash_N v rámci regcomp.c, ktoré možno zneužiť na neoprávnený prístup k informáciám alebo zneprístupnenie služby použitím regulárneho výrazu zakončeného s '\N{U+...}'.

Dátum prvého zverejnenia varovania

13. 11. 2017

CVE

CVE-2017-12837, CVE-2017-12883

Zasiahnuté systémy

Ubuntu 17.04, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS

Následky

Neprístupnosť služby, Neoprávnené vykonanie kódu, Neoprávnený prístup k informáciám

Odporúčania

Predmetnú zraniteľnosť možno opraviť aktualizáciou operačného systému: Ubuntu 17.04 (perl 5.24.1-2ubuntu1.1), Ubuntu 16.04 LTS (perl 5.22.1-9ubuntu0.2), Ubuntu 14.04 LTS(perl 5.18.2-2ubuntu1.3)

Zdroje

https://usn.ubuntu.com/usn/usn-3478-1/

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

Identifikátor

Microsoft Patch Tuesday, November 2017

Popis

Spoločnosť Microsoft vydala súbor aktualizácií, ktoré opravujú zraniteľnosti na rôzne produkty od spoločnosti Microsoft.

Dátum prvého zverejnenia varovania

14. 11. 2017

CVE

CVE-2017-11855, CVE-2017-11856, CVE-2017-11845, CVE-2017-11836, CVE-2017-11837, CVE-2017-11838, CVE-2017-11839, CVE-2017-11840, CVE-2017-11841, CVE-2017-11843, CVE-2017-11846, CVE-2017-11858, CVE-2017-11861, CVE-2017-11862, CVE-2017-11866, CVE-2017-11869, CVE-2017-11870, CVE-2017-11871, CVE-2017-11873, CVE-2017-11770, CVE-2017-11879, CVE-2017-11883, CVE-2017-11830, CVE-2017-11827, CVE-2017-11803, CVE-2017-11833, CVE-2017-11844, CVE-2017-11863, CVE-2017-11872, CVE-2017-11874, CVE-2017-11878, CVE-2017-11877, CVE-2017-11850, CVE-2017-11882, CVE-2017-11884, CVE-2017-11854, CVE-2017-11791, CVE-2017-11834, CVE-2017-11832, CVE-2017-11835, CVE-2017-11852, CVE-2017-11831, CVE-2017-11880, CVE-2017-11847, CVE-2017-11842, CVE-2017-11849, CVE-2017-11851, CVE-2017-11853, CVE-2017-11768, CVE-2017-11788, CVE-2017-8700, CVE-2017-11848, CVE-2017-11876

Zasiahnuté systémy

Produkty spoločnosti Microsoft

Následky

Neprístupnosť služby, Neoprávnený prístup k systému, Neoprávnené vykonanie škodlivého kódu

Odporúčania

Odporúčame aktualizovať všetky produkty spoločnosti Microsoft na aktuálnu verziu.

Zdroje

https://www.trustwave.com/Resources/SpiderLabs-Blog/Microsoft-Patch-Tuesday,-November-2017/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

New Banking Trojan IcedID

Popis

Malware IcedID manipuluje s webovými prehliadačmi a zameriava sa na systémy bánk, poskytovateľov mobilných služieb, webmail-ov a E-commerce systémy. Okrem štandardných vlastností trójskych koňov sa navyše dokáže šíriť prostredníctvom siete. Vytvára lokálne proxy a následne monitoruje online aktivitu používateľa. Samotný útok využíva webinjection a presmerovanie.

Dátum prvého zverejnenia varovania

13. 11. 2017

Vektor útoku

IcedID sa na cieľové zariadenia dostane prostredníctvom trójskeho koňa „Emotet“, ktorý sa šíri prostredníctvom e-mailového spamu so súbormi obsahujúcimi škodlivé makrá. IcedID vytvorí lokálne proxy, cez ktoré smeruje online prevádzku zariadenia. Prevádzka je smerovaná cez localhost (127.0.0.1) na porte 49157, na ktorom počúva škodlivý proces a relevantný obsah komunikácie posiela prostredníctvom SSL šifrovaného kanála na svoj riadiaci C&C server. IcedID využíva sofistikované presmerovanie na repliky dôležitých stránok (napr. bankové portály), ktoré zobrazuje URL pôvodnej stránky a správny SSL certifikát. Obeť zadá svoje prístupové dáta do repliky stránky a útočník preberie kontrolu nad prebiehajúcou reláciou. Na obídenie dodatočných bezpečnostných prvkov útočník používa princípy sociálneho inžinierstva.

Zasiahnuté systémy

Windows, webové prehliadače

Následky

Neprístupnosť služby, Neoprávnený prístup k častiam systému

Odporúčania

Odporúčame informovať používateľov o rizikách a spôsoboch identifikácie spamového obsahu a aktualizáciu webových prehliadačov na najnovšiu verziu.

Zdroje

https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
https://gbhackers.com/banking-trojan-icedid-evade-sandbox/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 4.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

79 zraniteľností USB v Linux Kerneli

Popis

Výskumníci spoločnosti Google objavili 79 zraniteľností USB ovládačov v Linux Kerneli.
Prvých 14 zraniteľností bolo odhalených pomocou nástroja syzkaller, ďalších 65 zraniteľností bolo odhalených neskôr pri výskume rovnakých subsystémov v USB ovládačoch.
Zraniteľnosti umožňujú útočníkovi získať priamy prístup k systému alebo zariadeniu. Stačí, ak je do USB portu vložený špeciálne upravený USB kľúč. Útočník tak nemusí byť fyzicky prítomný pri zariadení, stačí, ak sofistikovaným spôsobom zabezpečí, aby takýto USB kľúč vložil do zariadenia jeho používateľ.
Časť zraniteľností umožňuje útočníkovi vykonať útok, spočívajúci v zneprístupnení služby (DoS).

Dátum prvého zverejnenia varovania

Prvé zverejnenie 07. 11. 2017, aktualizované 14. 11. 2017

CVE

CVE-2017-16525, CVE-2017-16526, CVE-2017-16527, CVE-2017-16528, CVE-2017-16529, CVE-2017-16530, CVE-2017-16531, CVE-2017-16532, CVE-2017-16533, CVE-2017-16534, CVE-2017-16535, CVE-2017-16536, CVE-2017-16537, CVE-2017-16538, CVE-2017-16649, CVE-2017-16650, CVE-2017-16648, CVE-2017-16643, CVE-2017-16647, CVE-2017-16645, CVE-2017-16646, CVE-2017-16644

Zasiahnuté systémy

Linux Kernel

Následky

Neoprávnený prístup do systému, Zneprístupnenie služby

Odporúčania

V súvislosti s vyššie uvedenými zraniteľnosťami odporúčame dodržiavať nasledujúce opatrenia:

1. Pri manipulácii a používaní USB kľúčov, USB diskov alebo iných zariadení, ktoré sú k vášmu zariadeniu pripájané prostredníctvom USB portu dôsledne preverujte ich pôvod a obsah. Pri akejkoľvek podozrivej aktivite zašlite USB kľúč alebo zariadenie na kompletnú forenznú analýzu na pracovisko SK-CERT.
2. Nepoužívajte USB kľúče a zariadenia, ktoré pochádzajú z nepreverného zdroja (napr. nájdené, darované a pod.), na prenos citlivých informácií alebo v zariadeniach s obsahom citlivých informácií.
3. Udržujte svoje operačné systémy a zariadenia aktualizované na najnovšiu verziu.

Zdroje

https://nakedsecurity.sophos.com/2017/11/14/google-researcher-finds-79-linux-usb-vulnerabilities/amp/
https://github.com/google/syzkaller/blob/master/docs/linux/found_bugs_usb.md
http://www.openwall.com/lists/oss-security/2017/11/06/8

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-023