BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 11. 2017 – 28. 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-027

BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 11. 2017 – 28. 11. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Vulnerability in middleware.py in OpenStack Swauth

Popis

OpenStack Swauth obsahuje zraniteľnosť v middleware.py. Úložisko Swift objektov a proxy server ukladajú nehash-ované tokeny získané z autentifikačného mechanizmu do log súboru ako súčasť GET URI. Zraniteľnosť umožňuje útočníkom obídenie autentifikácie vložením tokenu do X-Auth-Token hlavičky novej požiadavky.

Dátum prvého zverejnenia varovania

22.11.2017 (posledná aktualizácia 28.11.2017)

CVE

CVE-2017-16613

Zasiahnuté systémy

OpenStack Swauth verzie 1.2.0

Následky

Neoprávnený prístup k systému

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutého produktu na najnovšiu verziu.

Zdroje

https://security-tracker.debian.org/tracker/CVE-2017-16613
http://www.securityfocus.com/bid/101926
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=882314

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

Identifikátor

Scarab ransomware spreading

Popis

Bezpečnostní analytici varujú pred hromadnou distribúciou ransomwaru pomocou e-mailového spamu šíreného prostredníctvom botnetu Necurs, ktorý sa v minulosti využil na šírenie ransomwarov Locky a Jaff. Ransomware Scarab sa primárne šíri na doménu najvyššej úrovne .com, ale analytici zaznamanali aj jeho šírenia na domény najvyššj úrovne v rámci Európy (Veľá Británia, Francúzsko, Nemecko).

Spamové e-maily s predmetom „Scanned from {názov výrobcu tlačiarní}“ obsahujú 7zip prílohu s VBScirpt downloaderom. Domény používané na download ransomwaru sú v spojení s predchádzajúcimi útokmi z botnetu Necurs.

Po inštalácii ransomware dotknuté súbory zašifruje, pridá príponu ‘.[suupport@protonmail.com].scarab’ a následne do priečinkov obsahujúcich dotknuté súbory pridá textový dokument obsahujúci pokyny k obnoveniu súborov. Primárnym komunikačným mechanizmom je e-mailová komunikácia, dokument bližšie nešpecifikuje požadovanú platbu v Bitcoinoch a len oznamuje, že výška platby závisí od rýchlosti odpovede obete. Ransomware Scarab demonštruje schopnosť invertovať zmeny ponukou bezplatného dešifrovania 3 súborov.

Podľa bezpečnostných expertov z AlienVault, je ransomware Scarab napriek intenzívnej distribučnej kampane detekovateľný väčšinou anti-malwarových softwarov.

Dátum prvého zverejnenia varovania

23. 11. 2017 (posledná aktualizácia 26.11.2017)

Následky

Zamedzenie prístupu k informáciám

Odporúčania

Odporúčame informovať používateľov o rizikách a spôsoboch identifikácie spamového obsahu a udržiavať antivírusovú databázu aktualizovanú. Navyše odporúčame vykonávať pravidelné zálohovanie dôležitých súborov na externé úložisko bez trvalého pripojenia k Vašim počítačom.

Zdroje

https://www.infosecurity-magazine.com/news/scarab-ransomware-necurs-spread/
https://thehackernews.com/2017/11/necrus-scarab-ransomware.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Security vulnerability of all versions of Samba from 4.0.0 onwards

Popis

Samba server pre zdieľanie priečinkov a súborov obsahuje bezpečnostné zraniteľnosti, ktoré neoprávnenému útočníkovi umožňujú prostredníctvom špecifických požiadaviek SMB1 spôsobiť pád servera alebo neoprávnené vykonanie kódu.
Špecifické požiadavky SMB1 možno využiť na modifikáciu obsahu dynamickej pamäte servera prostredníctvom nesprávne dealokovaného smerníka.

Dátum prvého zverejnenia varovania

21.11.2017 (posledná aktualizácia 23.11.2017)

CVE

CVE-2017-14746

Zasiahnuté systémy

Všetky verzie Samba 4.x pred verziou 4.7.3

Následky

Neprístupnosť služby, Neoprávnené vykonanie kódu, Neoprávnený prístup k informáciám

Odporúčania

Najpoužívanejšie Linuxové distribúcie už vydali bezpečnostné záplaty pre uvedenú zraniteľnosť. Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu svojich serverov.
Alternatívne riešenie spočíva vo vypnutí SAMBA 1 nastavením parametra „server min protocol = SMB2“ v sekcii [global] konfiguračného súbora smb.conf a následnom reštarte Samby.

Zdroje

https://andreafortuna.org/security/cve-2017-14746-you-need-to-patch-your-samba-as-soon-as-possible/
https://access.redhat.com/security/cve/cve-2017-14746
https://www.samba.org/samba/security/CVE-2017-14746.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Vulnerabilities in PowerDNS

Popis

Vybrané verzie softwarov PowerDNS Recursor a PowerDNS Authoritativeod výrobcu PowerDNS obsahujú viacero zraniteľností, ktoré by útočník mohol využiť na neoprávnenú manipuláciu s údajmi a obmedzenie až zneprístupnenie služby.
DNSSEC komponent PowerDNS Recursor-a môže prijať neplatne podpísané dáta. Útočník man-in-the-middle tak môže do systému vložiť neplatné dáta.
Niektoré operácie v rámci API komponentu PowerDNS Authoritative, ktoré majú dopad na stav serveru, sú povolené aj v prípade, že je API nakonfigurované do režimu len na čítanie. Útočník s platnými prihlasovacími údajmi môže vymazať cache pamäť a odoslať NOTIFY správu.
Nesprávne zobrazovanie qname DNS dopytov vo webovom rozhraní PowerDNS Recursor umožňuje útočníkovi vykonať injekciu HTML alebo Javascriptového kódu, vedúce k modifikácii webového rozhrania.
Nesprávne parsovanie DNSSEC v rámci PowerDNS Recursor útočník môže využiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.11.2017 (Posledná aktualizácia 28.11.2017)

CVE

CVE-2017-15090, CVE-2017-15091, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Zasiahnuté systémy

PowerDNS Recursor od verzie 4.0.0 po verziu 4.0.6, PowerDNS Authoritative po verziu 4.0.4 a verzie 3.4.11

Následky

Neoprávnená manipulácia s údajmi, Neprístupnosť služby

Odporúčania

PowerDNS vydal aktualizácie, ktoré riešia uvedené zraniteľnosti. Administrátorom odporúčame bezokladne vykonať aktualizáciu dotknutých softwarov.

Zdroje

https://www.theregister.co.uk/2017/11/28/powerdns_dnssec_bugs/