BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 12. 2019 - 10. 12. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	UNIX / LINUX VPN zraniteľnosť	Vysoká	**8.8**
02.	Accusoft ImageGear viacero zraniteľností	Vysoká	**8.8**
03.	Amazon Blink XT2 Sync Modules zraniteľnosti	Vysoká	**8.3**
04.	Django framework zraniteľnosť	Vysoká	**8.3**
05.	OpenBSD viacero zraniteľností	Vysoká	**7.8**
06.	Wireshark zraniteľnosť	Vysoká	**7.5**
07.	Thales DIS SafeNet Sentinel LDK License Manager Runtime zraniteľnosť	Vysoká	**7.3**
08.	Dell Command Configure zraniteľnosť	Vysoká	**7.1**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01380/2019/SK-CERT-283

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

UNIX / LINUX VPN zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti operačných systémov založených na UNIX/LINUX.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne upravených TCP paketov získať neoprávnený prístup k citlivým údajom s prevziať kontrolu nad VPN spojením (OpenVPN, WireGuard, IKEv2/IPSec).

Dátum prvého zverejnenia varovania

04.12.2019

CVE

CVE-2019-14899

Zasiahnuté systémy

Operačné systémy založené na UNIX/LINUX (Ubuntu, Debian, Fedora, Arch, OpenBSD, FreeBSD, Android, MacOS, iOS)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Bezpečnostné aktualizácie riešiace uvedenú zraniteľnosť doposiaľ neboli vydané.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame zapnúť funkciu "reverse path filtering", funkciu filtrovania IP adries "bogon" a tiež zapnúť šifrovanie veľkosti paketov.

Zdroje

https://seclists.org/oss-sec/2019/q4/122
https://seclists.org/oss-sec/2019/q4/123
https://seclists.org/oss-sec/2019/q4/124
https://securityaffairs.co/wordpress/94764/hacking/cve-2019-14899-vpn-flaw.html
https://www.bleepingcomputer.com/news/security/new-linux-vulnerability-lets-attackers-hijack-vpn-connections/
https://thehackernews.com/2019/12/linux-vpn-hacking.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Accusoft ImageGear viacero zraniteľností

Popis

Spoločnosť Accusoft vydala aktualizáciu na svoj produkt ImageGear, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených PNG a TIFF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2019

CVE

CVE-2019-5076, CVE-2019-5083

Zasiahnuté systémy

Accusoft ImageGear 19.3.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-5083
https://nvd.nist.gov/vuln/detail/CVE-2019-5076
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0875
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0865

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Amazon Blink XT2 Sync Modules zraniteľnosti

Popis

Spoločnosť Amazon vydala bezpečnostnú aktualizáciu na svoju IP kameru Blink XT2 Sync Modules, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2019

CVE

CVE-2019-3983, CVE-2019-3984, CVE-2019-3985, CVE-2019-3986, CVE-2019-3987, CVE-2019-3988, CVE-2019-3989

Zasiahnuté systémy

Amazon Blink XT2 Sync Module verzie staršie ako 2.13.11

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.tenable.com/security/research/tra-2019-51

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Django framework zraniteľnosť

Popis

Vývojári webového frameworku Django vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

02.12.2019

CVE

CVE-2019-19118

Zasiahnuté systémy

Django verzie staršie ako 2.1.15 a 2.2.8

Následky

Eskalácia privilégií

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na frameworku Django v zraniteľných verziách. V prípade, že áno, vykonajte aktualizáciu frameworku.

Zdroje

https://www.djangoproject.com/weblog/2019/dec/02/security-releases/
https://nvd.nist.gov/vuln/detail/CVE-2019-19118

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

Identifikátor

OpenBSD viacero zraniteľností

Popis

Vývojári OpenBSD vydali aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

04.12.2019

CVE

CVE-2019-19519, CVE-2019-19520, CVE-2019-19521, CVE-2019-19522

Zasiahnuté systémy

OpenBSD 6.5 a 6.6

Následky

Eskalácia privilégií
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://blog.qualys.com/laws-of-vulnerabilities/2019/12/04/openbsd-multiple-authentication-vulnerabilities
https://seclists.org/oss-sec/2019/q4/120
https://exchange.xforce.ibmcloud.com/vulnerabilities/172581
https://exchange.xforce.ibmcloud.com/vulnerabilities/172582
https://exchange.xforce.ibmcloud.com/vulnerabilities/172583
https://exchange.xforce.ibmcloud.com/vulnerabilities/172584
https://www.zdnet.com/article/openbsd-patches-severe-authentication-bypass-privilege-escalation-vulnerabilities/
https://thehackernews.com/2019/12/openbsd-authentication-vulnerability.html
https://www.qualys.com/2019/12/04/cve-2019-19521/authentication-vulnerabilities-openbsd.txt

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

Identifikátor

Wireshark zraniteľnosť

Popis

Vývojári nástroja na analýzu sieťovej prevádzky Wireshark vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente CMS dissector je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

04.12.2019

CVE

CVE-2019-19553

Zasiahnuté systémy

Wireshark verzie staršie ako 3.0.7 a 2.6.13

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2019-22.html
https://nvd.nist.gov/vuln/detail/CVE-2019-19553

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Thales DIS SafeNet Sentinel LDK License Manager Runtime zraniteľnosť

Popis

Spoločnosť Thales DIS vydala bezpečnostnú aktualizáciu na svoj produkt SafeNet Sentinel LDK License Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

05.12.2019

CVE

CVE-2019-18232

Zasiahnuté systémy

Thales DIS SafeNet Sentinel LDK License Manager Runtime verzie staršie ako 7.101

Následky

Eskalácia privilégií
Vykonanie škodlivého kódu
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-339-01

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

Identifikátor

Dell Command Configure zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt Dell Command Configure, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

05.12.2019

CVE

CVE-2019-18575

Zasiahnuté systémy

Dell Command Configure verzie staršie ako 4.2.1

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.dell.com/support/article/sk/sk/skbsd1/SLN319715
https://exchange.xforce.ibmcloud.com/vulnerabilities/172718