BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 09. 2018 - 02. 10. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Netgate pfSense Command Injection Vulnerability	Vysoká	**8.8**
02.	Flatpak D-Bus Proxy Sandbox Escape Vulnerability	Vysoká	**8.8**
03.	Foxit Reader and Foxit PhantomPDF Multiple Vulnerabilities	Vysoká	**8.8**
04.	Cisco IOS and IOS XE Multiple Vulnerabilities	Vysoká	**8.6**
05.	Linux Kernel Multiple Vulnerabilities	Vysoká	**7.8**
06.	Telegram Leaking IP Vulnerability	Stredná	**5.3**

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:
02049/2018/TS/OKB-151

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

Identifikátor

Netgate pfSense Command Injection Vulnerability

Popis

Spoločnosť Netgate vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produkte pfSense.
Zraniteľnosť v komponente WebGUI nachádzajúca sa vo funkcii dhcp_relinquish_lease() definovanej v status_interfaces.php spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia HTTP POST parametrov mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.09.2018

CVE

CVE-2018-16055

Zasiahnuté systémy

Netgate pfSense verzie 2.3 (.0, .1, .2, .3, .3-p1, .4, .4-p1, .5, .5-p1, .5-p2)
Netgate pfSense verzie 2.4 (.0, .1, .2, .2-p1, .3, .3-p1)

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.pfsense.org/security/advisories/pfSense-SA-18_08.webgui.asc
https://tools.cisco.com/security/center/viewAlert.x?alertId=58967

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

Identifikátor

Flatpak D-Bus Proxy Sandbox Escape Vulnerability

Popis

Vývojári platformy pre virtualizáciu aplikácií Flatpak vydali bezpečnostné aktualizácie pre svoj produkt, ktoré opravujú bezpečnostnú zraniteľnosť v komponente D-Bus Proxy.
Zraniteľnosť nachádzajúca sa v dbus-proxy/flatpak-proxy.c spočíva v nedostatočnej implementácii mechanizmov autentifikácie a lokálny autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených D-Bus správ mohol zneužiť na únik zo sandboxového prostredia a získanie úplnej kontroly nad rozhraním D-Bus.

Dátum prvého zverejnenia varovania

26.09.2018

CVE

CVE-2018-6560

Zasiahnuté systémy

Flatpak verzie 0.8.0 až 0.8.8
Flatpak verzie 0.9.1 až 0.9.12, 0.9.98, 0.9.98.1, 0.9.98.2, 0.9.99
Flatpak verzie 0.10.0 až 0.10.2.1)

Následky

Neoprávnený prienik do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/flatpak/flatpak/commit/52346bf187b5a7f1c0fe9075b328b7ad6abe78f6
https://tools.cisco.com/security/center/viewAlert.x?alertId=58963

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

Identifikátor

Foxit Reader and Foxit PhantomPDF Multiple Vulnerabilities

Popis

Spoločnosť Foxit Software vydala bezpečnostné aktualizácie na svoje produkty Foxit Reader a Foxit PhantomPDF, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov vo funkcii setInterval() a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.09.2018

CVE

CVE-2018-17625, CVE-2018-17706, CVE-2018-17615, CVE-2018-17616, CVE-2018-17617, CVE-2018-17618, CVE-2018-17619, CVE-2018-17620, CVE-2018-17621, CVE-2018-17622, CVE-2018-17623, CVE-2018-17624

Zasiahnuté systémy

Foxit Reader 9.2.0.9297 a staršie
Foxit PhantomPDF 9.2.0.9297 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php
https://blog.talosintelligence.com/2018/10/foxit-pdf-reader-multiple-vulnerabilities.html
https://www.zerodayinitiative.com/advisories/ZDI-18-1094/
https://www.zerodayinitiative.com/advisories/ZDI-18-1094/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco IOS and IOS XE Multiple Vulnerabilities

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produktoch Cisco IOS a IOS XE.
Najzávažnejšie zraniteľnosti spočívajú v nesprávnom spracovaní SIP, HTTP a IPv6 paketov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených paketov mohol zneužiť na znepristupnenie služby.
Ostatné zraniteľnosti by útočník mohol zneužiť na znepristupnenie služby a neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

26.09.2018

CVE

CVE-2018-0197, CVE-2018-0466, CVE-2018-0467, CVE-2018-0469, CVE-2018-0470, CVE-2018-0471, CVE-2018-0473, CVE-2018-0475, CVE-2018-0476, CVE-2018-0477, CVE-2018-0480, CVE-2018-0481, CVE-2018-0485, CVE-2018-15368, CVE-2018-15369, CVE-2018-15371, CVE-2018-15372, CVE-2018-15373, CVE-2018-15374, CVE-2018-15375, CVE-2018-15376, CVE-2018-15377

Zasiahnuté systémy

Cisco IOS and IOS XE Software

Následky

Znepristupnenie služby, Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-cdp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-digsig
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-ir800-memwrite
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-macsec
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-pnp-memleak
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-shell-access
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-tacplus
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-vtp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-cdp-memleak
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-cmp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-errdisable
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-iosxe-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-ipv6hbh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-ptp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-sip-alg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-sm1t3e3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-webdos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-webuidos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-ospfv3-dos

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

Identifikátor

Linux Kernel Multiple Vulnerabilities

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza vo funkcii create_elf_tables a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a úplné narušenie dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.
Druhá zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie vo funkcii chap_server_compute_md5() a vzdialený neautentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.10.2018

CVE

CVE-2018-14634

Zasiahnuté systémy

Linux Kernel

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58964

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Telegram Leaking IP Vulnerability

Popis

Vývojári komunikačnej platformy Telegram vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viaceré bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi identifikovať IP adresu napadnutého zariadenia.

Dátum prvého zverejnenia varovania

30.11.-0001

CVE

CVE-2018-17780, CVE-2018-17613

Zasiahnuté systémy

Telegram Desktop 1.3.14; 1.3.16 alpha
Telegram 3.3.0.0 WP8.1 pre Windows

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://thehackernews.com/2018/09/hack-telegram-messenger.html?m=1
https://www.theregister.co.uk/2018/10/01/telegram_bug_ip_addresses/
https://nvd.nist.gov/vuln/detail/CVE-2018-17780
https://www.inputzero.io/2018/09/bug-bounty-telegram-cve-2018-17780.html
https://nvd.nist.gov/vuln/detail/CVE-2018-17613
https://www.inputzero.io/2018/09/telegram-share-password-in-cleartext.html