BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 06. 2020 - 16. 06. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe produkty viacero zraniteľností	Vysoká	**8.8**
02.	WordPress viacero zraniteľností	Vysoká	**8.8**
03.	Netgear R6700 viacero zero-day zraniteľností	Vysoká	**8.8**
04.	Moxa EDR-G902 a G903 zraniteľnosť	Vysoká	**8.8**
05.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
06.	Zraniteľnosti produktov Lenovo	Vysoká	**8.4**
07.	IBM Spectrum Protect Plus zraniteľnosti	Vysoká	**8.1**
08.	Intel produkty viacero zraniteľností	Vysoká	**7.9**
09.	ConnectWise Automate API zraniteľnosť	Vysoká	**7.8**
10.	Docker desktop zraniteľnosť	Vysoká	**7.8**
11.	OSIsoft PI Web API 2019 zraniteľnosť	Vysoká	**7.7**
12.	GnuTLS zraniteľnosť	Vysoká	**7.4**

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:
01439/2020/SK-CERT-151

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 06. 2020 - 16. 06. 2020

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

Identifikátor

Adobe produkty viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti v produktoch Flash Player a Framemaker umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2020-9633, CVE-2020-9634, CVE-2020-9635, CVE-2020-9636, CVE-2020-9643, CVE-2020-9644, CVE-2020-9645, CVE-2020-9647, CVE-2020-9648, CVE-2020-9651

Zasiahnuté systémy

Adobe Framemaker verzie staršie ako 2019.0.6
Adobe Experience Manager verzie staršie ako 6.5.5.0 a 6.4.8.1
Adobe Flash Player verzie staršie ako 32.0.0.387

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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://helpx.adobe.com/security/products/flash-player/apsb20-30.html
https://helpx.adobe.com/security/products/experience-manager/apsb20-31.html
https://helpx.adobe.com/security/products/framemaker/apsb20-32.html
https://threatpost.com/adobe-warns-critical-flaws-flash-player-framemaker/156417/
https://www.cisecurity.org/advisory/a-vulnerability-in-adobe-flash-player-could-allow-for-arbitrary-code-execution-apsb20-30_2020-080/

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

Identifikátor

WordPress viacero zraniteľností

Popis

Vývojári redakčného systému WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi prostredníctvom XSS útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.06.2020

CVE

CVE-2020-4046, CVE-2020-4047, CVE-2020-4048, CVE-2020-4049, CVE-2020-4050

Zasiahnuté systémy

WordPress verzie staršie ako 5.4.2

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress v zraniteľnej verzii. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
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://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/
https://exchange.xforce.ibmcloud.com/vulnerabilities/183390
https://exchange.xforce.ibmcloud.com/vulnerabilities/183391
https://exchange.xforce.ibmcloud.com/vulnerabilities/183387
https://exchange.xforce.ibmcloud.com/vulnerabilities/183388
https://exchange.xforce.ibmcloud.com/vulnerabilities/183389

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

Identifikátor

Netgear R6700 viacero zero-day zraniteľností

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v smerovačoch Netgear R6700.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.06.2020

CVE

-

Zasiahnuté systémy

Netgear R6700

Následky

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

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedené zraniteľnosti doposiaľ nebola vydaná. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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.zerodayinitiative.com/advisories/ZDI-20-703/
https://www.zerodayinitiative.com/advisories/ZDI-20-704/
https://www.zerodayinitiative.com/advisories/ZDI-20-705/
https://www.zerodayinitiative.com/advisories/ZDI-20-708/
https://www.zerodayinitiative.com/advisories/ZDI-20-709/
https://www.zerodayinitiative.com/advisories/ZDI-20-713/
https://www.zerodayinitiative.com/advisories/ZDI-20-711/
https://www.zerodayinitiative.com/advisories/ZDI-20-706/
https://www.zerodayinitiative.com/advisories/ZDI-20-712/
https://www.zerodayinitiative.com/advisories/ZDI-20-707/

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

Identifikátor

Moxa EDR-G902 a G903 zraniteľnosť

Popis

Spoločnosť Moxa vydala aktualizáciu na svoje smerovače EDR-G902 a G903, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.06.2020

CVE

-

Zasiahnuté systémy

Moxa EDR-G902 Series verzie staršie ako 5.5
Moxa EDR-G903 Series verzie staršie ako 5.5

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://www.moxa.com/en/support/support/security-advisory/edr-g902-g903-series-secure-routers-vulnerabilities

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.06.2020

CVE

CVE-2020-6505, CVE-2020-6506, CVE-2020-6507

Zasiahnuté systémy

Google Chrome verzie staršie ako 83.0.4103.106

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_15.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/183401

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti produktov Lenovo

Popis

Spoločnosť Lenovo vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému..

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2019-14561, CVE-2019-14562, CVE-2020-0528, CVE-2020-0529, CVE-2020-8320, CVE-2020-8321, CVE-2020-8322, CVE-2020-8323, CVE-2020-8331, CVE-2020-8334, CVE-2020-8336

Zasiahnuté systémy

Notebooky a PC Lenovo, kompletný zoznam zasiahnutých produktov je dostupný na
https://support.lenovo.com/us/en/product_security/PS500328

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.lenovo.com/us/en/product_security/LEN-30042
https://exchange.xforce.ibmcloud.com/vulnerabilities/183177

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

Identifikátor

IBM Spectrum Protect Plus zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Spectrum Protect Plus, ktorá opravuje bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.06.2020

CVE

CVE-2020-4216, CVE-2020-4469, CVE-2020-4470, CVE-2020-4471

Zasiahnuté systémy

IBM Spectrum Protect Plus verzie staršie ako 10.1.6

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.ibm.com/support/pages/node/6221358
https://www.ibm.com/support/pages/node/6221332
https://www.tenable.com/security/research/tra-2020-37
https://exchange.xforce.ibmcloud.com/vulnerabilities/181724

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel produkty viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť vo firmvéri SSD diskov umožňuje lokálnemu, autentifikovanému útočníkovi získať prístup k citlivým údajom a zraniteľnosti v BIOSe procesorov Intel Core umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a tiež spôsobiť zneprístupnenie služieb a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.06.2020

CVE

CVE-2020-0527, CVE-2020-0528, CVE-2020-0529, CVE-2020-0543

Zasiahnuté systémy

Intel® SSD D3-S4510 Series M.2 FF verzie firmvéru staršie ako XC311120
Intel® SSD DC P4510 Series (U.2 only) verzie firmvéru staršie ako VDV10170
Intel® SSD DC P4510 Series OPAL verzie firmvéru staršie ako VDV10170
Intel® SSD DC P4610 Series verzie firmvéru staršie ako VDV10170
Intel® SSD DC P4610 Series OPAL verzie firmvéru staršie ako VDV10170
Intel® SSD DC P4618 Series verzie firmvéru staršie ako VDV10170
Intel® SSD DC P4511 Series (m.2 only) verzie firmvéru staršie ako VCV10370
Procesory Intel® Core™ 7 až 10 generácie
Procesory Intel, kompletný zoznam zasiahnutých produktov je dostupný na https://software.intel.com/security-software-guidance/processors-affected-transient-execution-attack-mitigation-product-cpu-model

Následky

Eskalácia privilégií
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00322.html https://thehackernews.com/2020/06/intel-sgaxe-crosstalk-attacks.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00320.html https://exchange.xforce.ibmcloud.com/vulnerabilities/183185 https://exchange.xforce.ibmcloud.com/vulnerabilities/183174 https://exchange.xforce.ibmcloud.com/vulnerabilities/183173 https://support.lenovo.com/us/en/product_security/LEN-30040 https://sgaxe.com/

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

Identifikátor

ConnectWise Automate API zraniteľnosť

Popis

Spoločnosť ConnectWise vydala bezpečnostnú aktualizáciu svojho produktu Automate, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v API rozhraní umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.06.2020

CVE

-

Zasiahnuté systémy

ConnectWise Automate

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://www.connectwise.com/company/trust#tab1
https://www.theregister.com/2020/06/12/connectwise_security/

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

Identifikátor

Docker desktop zraniteľnosť

Popis

Vývojári Docker vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

22.05.2020

CVE

CVE-2020-11492

Zasiahnuté systémy

Docker desktop verzie staršie ako 2.3.0.2

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-20-715/
https://nvd.nist.gov/vuln/detail/CVE-2020-11492
https://www.pentestpartners.com/security-blog/docker-desktop-for-windows-privesc-cve-2020-11492/
https://nakedsecurity.sophos.com/2020/05/26/docker-desktop-danger-discovered-patch-now/
https://www.bleepingcomputer.com/news/security/docker-fixes-windows-client-bug-letting-programs-run-as-system/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

OSIsoft PI Web API 2019 zraniteľnosť

Popis

Spoločnosť OSIsoft vydala bezpečnostnú aktualizáciu svojho produktu PI Web API 2019, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňujú vzdialenému, autentifikovanému útočníkovi prostredníctvom XSS útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.06.2020

CVE

CVE-2020-12021

Zasiahnuté systémy

OSIsoft PI Web API 2019 verzie staršie ako SP1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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.us-cert.gov/ics/advisories/icsa-20-163-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GnuTLS zraniteľnosť

Popis

Vývojári knižnice GnuTLS vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom MITM útoku získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.06.2020

CVE

CVE-2020-13777

Zasiahnuté systémy

GnuTLS verzie staršie ako 3.6.14

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú knižnicu GnuTLS. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.theregister.com/2020/06/10/gnutls_patches_security_hole/
https://gitlab.com/gnutls/gnutls/-/issues/1011
https://nvd.nist.gov/vuln/detail/CVE-2020-13777
https://access.redhat.com/security/cve/cve-2020-13777