BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 03. 2023 - 14. 03. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	NETGEAR CAX Modemy - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Foxit PDF - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
04.	Zoho ManageEngine - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	Jenkins produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	Cisco produkty - dve bezpečnostné zraniteľnosti	Vysoká	**8.6**
07.	HPE Integrated Lights-Out - bezpečnostná zraniteľnosť	Vysoká	**8.3**
08.	Parallels Desktop - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
09.	QlikView - bezpečnostná zraniteľnosť	Vysoká	**7.6**
10.	Veeam Backup & Replication - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	Apache HTTP Server - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**

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:
01794/2022/SK-CERT-1061

BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 03. 2023 - 14. 03. 2023

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

Identifikátor

NETGEAR CAX Modemy - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostné aktualizácie na modemy CAX30 a CAX30S, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.03.2023

CVE

CVE-2022-43654

Zasiahnuté systémy

CAX30 vo verzii firmvéru staršej ako 2.1.3.10
CAX30S vo verzii firmvéru staršej ako 2.1.3.10

Následky

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

Odporúčania

Administrátorom a používateľom 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://kb.netgear.com/000065527/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-Cable-Modem-Routers-PSV-2022-0208
https://www.zerodayinitiative.com/advisories/ZDI-23-214/

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.03.2023

CVE

CVE-2023-1213, CVE-2023-1214, CVE-2023-1215, CVE-2023-1216, CVE-2023-1217, CVE-2023-1218, CVE-2023-1219, CVE-2023-1220, CVE-2023-1221, CVE-2023-1222, CVE-2023-1223, CVE-2023-1224, CVE-2023-1225, CVE-2023-1226, CVE-2023-1227, CVE-2023-1228, CVE-2023-1229, CVE-2023-1230, CVE-2023-1231, CVE-2023-1232, CVE-2023-1233, CVE-2023-1234, CVE-2023-1235, CVE-2023-1236

Zasiahnuté systémy

Google Chrome pre Linux a Mac vo verzii staršej ako 111.0.5563.64
Google Chrome pre Windows vo verzii staršej ako 111.0.5563.64/.65

Následky

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

Odporúčania

Administrátorom a používateľom 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/2023/03/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/249425

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

Identifikátor

Foxit PDF - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.03.2023

CVE

CVE-2023-27329, CVE-2023-27330, CVE-2023-27331

Zasiahnuté systémy

Foxit PDF Editor vo verzii staršej ako 11.2.5
Foxit PDF Reader vo verzii staršej ako 12.1.1
Foxit PDF Editor vo verzii staršej ako 12.1.1

Následky

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

Odporúčania

Administrátorom a používateľom 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://www.zerodayinitiative.com/advisories/ZDI-23-227/

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

Identifikátor

Zoho ManageEngine - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoho vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.03.2023

CVE

CVE-2023-26600, CVE-2023-26601

Zasiahnuté systémy

ServiceDesk Plus vo verzii staršej ako 14104
ServiceDesk Plus MSP vo verzii staršej ako 14001
SupportCenter Plus vo verzii staršej ako 14001
AssetExplorer vo verzii staršej ako 6988

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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.manageengine.com/products/service-desk/CVE-2023-26601.html
https://www.manageengine.com/products/service-desk/CVE-2023-26600.html
https://www.zerodayinitiative.com/advisories/ZDI-23-229/
https://www.zerodayinitiative.com/advisories/ZDI-23-230/

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

Identifikátor

Jenkins produkty - viacero bezpečnostných zraniteľností

Popis

Vývojári servera pre automatizáciu Jenkins vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored XSS (Cross-Site Scripting) útokú získať neoprávnený prístuo k citlivým údajom.
Ostatné zraniteľnosti by vzdialený útočník mohol zneužíť na zneprístupnenie služby, získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme.

Dátum prvého zverejnenia varovania

08.03.2023

CVE

CVE-2023-24998, CVE-2023-27898, CVE-2023-27899, CVE-2023-27900, CVE-2023-27901, CVE-2023-27902, CVE-2023-27903, CVE-2023-27904, CVE-2023-27905

Zasiahnuté systémy

Jenkins weekly vo verzii staršej ako 2.394
Jenkins LTS vo verzii staršej ako 2.375.4 alebo 2.387.1
update-center2 vo verzii staršej ako 3.15

Následky

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

Odporúčania

Administrátorom a používateľom 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.jenkins.io/security/advisory/2023-03-08/
https://exchange.xforce.ibmcloud.com/vulnerabilities/249545
https://securityaffairs.com/143237/security/jenkins-cloudbees-flaws.html

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

Identifikátor

Cisco produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.03.2023

CVE

CVE-2023-20049, CVE-2023-20064

Zasiahnuté systémy

IOS XR Software 6.5 vo všetkých verziách
IOS XR Software 6.6 vo všetkých verziách
IOS XR Software 7 vo všetkých verziách
IOS XR Software 7.1 vo všetkých verziách
IOS XR Software 7.3 vo všetkých verziách
IOS XR Software 7.4 vo všetkých verziách
IOS XR Software 7.5 vo verzii staršej ako 7.5.3
IOS XR Software 7.6 vo verzii staršej ako 7.6.2
IOS XR Software 7.7 a vyššie vo verzii staršej ako 7.7.1
ASR 9000 Series Aggregation Services Routers (64-bit) s IOS XR Software vo verzii staršej ako 7.9.1
IOSXRWBD s IOS XR Software vo verzii staršej ako 7.9.1
IOS XRv 9000 Routers s IOS XR Software vo verzii staršej ako 7.9.1
NCS 540 and 560 Series Routers s IOS XR Software vo verzii staršej ako 7.6.1
NCS 1001, 1002, and 1004 Series Routers s IOS XR Software vo verzii staršej ako 7.9.1
NCS 5000 Series Routers s IOS XR Software vo verzii staršej ako 7.7.1
NCS 5500 and 5700 Series Routerss IOS XR Software vo verzii staršej ako 7.6.1
NCS 6000 Series Routers s IOS XR Software vo všetkých verziách

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq

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

Identifikátor

HPE Integrated Lights-Out - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoju technológiu pre manažment serverov Integrated Lights-Out, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente vykonať Stored XSS (Cross-Site Scripting) útok a následne získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

13.03.2023

CVE

CVE-2023-28083

Zasiahnuté systémy

HPE Integrated Lights-Out 6 (iLO 6) vo verzii firmvéru staršej ako v1.20
HPE Integrated Lights-Out 5 (iLO 5) vo verzii firmvéru staršej ako v2.78
HPE Integrated Lights-Out 4 (iLO 4) vo verzii firmvéru staršej ako v2.82

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Parallels Desktop - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Parallels vydala bezpečnostnú aktualizáciu na svoj virtualizačný softvér Parallels Desktop, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora na guest systéme eskalovať svoje privilégiá a následne vykonať škodlivý kód v kontexte hypervisora.

Dátum prvého zverejnenia varovania

07.03.2023

CVE

CVE-2023-27323, CVE-2023-27324, CVE-2023-27325, CVE-2023-27326, CVE-2023-27328

Zasiahnuté systémy

Parallels Desktop vo verzii staršej ako 18.1.1 (53328)

Následky

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

Odporúčania

Administrátorom a používateľom 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://kb.parallels.com/125013
https://www.zerodayinitiative.com/advisories/ZDI-23-217/
https://www.zerodayinitiative.com/advisories/ZDI-23-218/
https://www.zerodayinitiative.com/advisories/ZDI-23-219/
https://www.zerodayinitiative.com/advisories/ZDI-23-220/
https://www.zerodayinitiative.com/advisories/ZDI-23-221/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

QlikView - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qlik vydala bezpečnostnú aktualizáciu na svoju analytickú platformu QlikView, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom XSS (Cross-Site Scripting) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

08.03.2023

CVE

CVE-2022-42248

Zasiahnuté systémy

QlikView vo verzii staršej ako 12.70 SR2

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom 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 získanie prístupu k citlivým údajom 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://exchange.xforce.ibmcloud.com/vulnerabilities/249430

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

Identifikátor

Veeam Backup & Replication - bezpečnostná zraniteľnosť

Popis

Spoločnosť Veeam vydala bezpečnostnú aktualizáciu na svoj produkt Veeam Backup & Replication, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky na port TCP 9401 získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

08.03.2023

CVE

CVE-2023-27532

Zasiahnuté systémy

Veeam Backup & Replication

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, výrobca odporúča blokovať vonkajší prístup na port TCP 9401 prostredníctvom bezpečnostných prvkov sieťovej infraštruktúry (firewall).
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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.bleepingcomputer.com/news/security/veeam-fixes-bug-that-lets-hackers-breach-backup-infrastructure/
https://www.veeam.com/kb4424

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

Identifikátor

Apache HTTP Server - dve bezpečnostné zraniteľnosti

Popis

Vývojári Apache HTTP Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti nachádzajúce sa v mod_proxy a mod_proxy_uwsgi spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávený prístup k citlivým údajom a obísť mechanizmy riadenia prístupu.

Dátum prvého zverejnenia varovania

07.03.2023

CVE

CVE-2023-25690, CVE-2023-27522

Zasiahnuté systémy

Apache HTTP Server vo verzii staršej ako 2.4.56

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://httpd.apache.org/security/vulnerabilities_24.html
https://access.redhat.com/security/cve/cve-2023-25690
https://www.securitynewspaper.com/2023/03/13/two-very-critical-vulnerabilities-patched-in-new-apache-http-server-update/