BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 04. 2023 - 02. 05. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apache Superset - bezpečnostná zraniteľnosť	Vysoká	**8.9**
02.	Scada-LTS - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Arista EOS - bezpečnostná zraniteľnosť	Vysoká	**8.8**
04.	cPanel - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Google Cloud Platform ESPv2 - bezpečnostná zraniteľnosť	Vysoká	**8.2**
06.	BOSCH B420 - bezpečnostná zraniteľnosť	Vysoká	**7.6**
07.	Progress Flowmon - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
08.	HCL Workload Automation - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
09.	Payload CMS - bezpečnostná zraniteľnosť	Vysoká	**7.4**
10.	IBM Watson Machine Learning on Cloud Pak for Data - bezpečnostná zraniteľnosť	Vysoká	**7.1**
11.	HPE ProLiant RL300 - bezpečnostná zraniteľnosť	Stredná	**6.1**
12.	Cisco Prime Collaboration Deployment - bezpečnostná zraniteľnosť	Stredná	**6.1**

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:
01794/2022/SK-CERT-1119

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.9**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Superset - bezpečnostná zraniteľnosť

Popis

Vývojári aplikácie Apache Superset vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného SECRET_KEY s predvolenou hodnotou a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-27524

Zasiahnuté systémy

Apache Superset vo verzii staršej ako 2.1.0

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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://nvd.nist.gov/vuln/detail/CVE-2023-27524
https://www.openwall.com/lists/oss-security/2023/04/24/2
https://thehackernews.com/2023/04/apache-superset-vulnerability-insecure.html

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

Identifikátor

Scada-LTS - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Scada-LTS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.04.2023

CVE

CVE-2015-1179

Zasiahnuté systémy

Scada-LTS vo verzii staršej ako 2.7.4.1

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
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.cisa.gov/news-events/ics-advisories/icsa-23-115-02

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

Identifikátor

Arista EOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Arista vydala bezpečnostné aktualizácie na svoj produkt Arista EOS, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.04.2023

CVE

CVE-2023-24512

Zasiahnuté systémy

Arista EOS produkty vo verzii staršej ako 4.29.2F
Arista EOS produkty vo verzii staršej ako 4.28.6M
Arista EOS produkty vo verzii staršej ako 4.27.9M
Arista EOS produkty vo verzii staršej ako 4.26.10M

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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.arista.com/en/support/advisories-notices/security-advisory/17250-security-advisory-0086
https://exchange.xforce.ibmcloud.com/vulnerabilities/253835

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

Identifikátor

cPanel - bezpečnostná zraniteľnosť

Popis

Spoločnosť cPanel vydala bezpečnostnú aktualizáciu na svoj rovnomenný produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom a do systému.

Dátum prvého zverejnenia varovania

27.04.2023

CVE

CVE-2023-29489

Zasiahnuté systémy

cPanel vo verzii staršej ako 11.109.9999.116

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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://blog.assetnote.io/2023/04/26/xss-million-websites-cpanel/
https://nvd.nist.gov/vuln/detail/CVE-2023-29489
https://forums.cpanel.net/threads/cpanel-tsr-2023-0001-full-disclosure.708949/
https://www.securitynewspaper.com/2023/04/27/you-dont-have-to-be-a-super-hacker-to-hack-into-milliones-of-websites-this-cpanel-flaw-makes-it-easy-for-anyone/

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

Identifikátor

Google Cloud Platform ESPv2 - bezpečnostná zraniteľnosť

Popis

Vývojári service proxy esp-v2 vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-30845

Zasiahnuté systémy

esp-v2 vo verzii staršej ako 2.43.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://github.com/GoogleCloudPlatform/esp-v2/security/advisories/GHSA-6qmp-9p95-fc5f
https://exchange.xforce.ibmcloud.com/vulnerabilities/253907

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

Identifikátor

BOSCH B420 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti ethernetového komunikačného modulu B420.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2022-47648

Zasiahnuté systémy

BOSCH B420 vo všetkých verziách (EoL)

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, výrobca odporúča prejsť na modul B426 bez známych zraniteľností. V prípade, že prechod na novší modul nie je možný, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-341298-bt.html
https://nvd.nist.gov/vuln/detail/CVE-2022-47648

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

Identifikátor

Progress Flowmon - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Progress vydala bezpečnostnú aktualizáciu na svoj nástroj na monitorovanie sietí Flowmon, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej URL požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.04.2023

CVE

CVE-2023-26100, CVE-2023-26101

Zasiahnuté systémy

Progress Flowmon Packet Investigator vo verzii staršej ako 12.1.0

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://www.redpacketsecurity.com/progress-flowmon-os-cross-site-scripting-cve-2023-26100/
https://www.redpacketsecurity.com/progress-flowmon-os-directory-traversal-cve-2023-26101/

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

Identifikátor

HCL Workload Automation - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť HCL Software vydala bezpečnostné aktualizácie na svoj produkt Workload Automation, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného XML dokumentu získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-28008, CVE-2023-28009

Zasiahnuté systémy

HCL Workload Automation vo verzii staršej ako 9.5.0.6
HCL Workload Automation vo verzii staršej ako 10.1.0.1

Následky

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://exchange.xforce.ibmcloud.com/vulnerabilities/253894

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

Identifikátor

Payload CMS - bezpečnostná zraniteľnosť

Popis

Vývojári redakčného systému Payload CMS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-30843

Zasiahnuté systémy

Payload CMS vo verzii staršej ako 1.7.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Payload CMS v zraniteľnej verzii. V prípade, že áno, administrátorom 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://github.com/payloadcms/payload/security/advisories/GHSA-35jj-vqcf-f2jf

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

Identifikátor

IBM Watson Machine Learning on Cloud Pak for Data - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt atson Machine Learning on Cloud Pak for Data, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-30444

Zasiahnuté systémy

IBM Watson Machine Learning on CP4D vo verzii staršej ako 4.6

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://exchange.xforce.ibmcloud.com/vulnerabilities/253350

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HPE ProLiant RL300 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt ProLiant RL300, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.04.2023

CVE

CVE-2023-28092

Zasiahnuté systémy

System ROM v1.20 or later
Integrated Lights-Out 6 (iLO 6) v.1.35 or later

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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=hpesbhf04472en_us

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Prime Collaboration Deployment - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Prime Collaboration Deployment, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2023-20060

Zasiahnuté systémy

Cisco Prime Collaboration Deployment vo verzii staršej ako 14SU3 (Máj 2023)

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pcd-xss-jDXpjm7
https://www.bleepingcomputer.com/news/security/cisco-discloses-xss-zero-day-flaw-in-server-management-tool/

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-1119