BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 10. 2023 - 31. 10. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	SICK Flexi Soft Gateway - kritická bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Roundcube - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Kubernetes ingress-nginx - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
06.	Apple produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
07.	Tenda W18E - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
08.	Home Assistant Companion App for iOS - bezpečnostná zraniteľnosť	Vysoká	**8.6**
09.	IBM Security Verify Governance - viacero bezpečnostných zraniteľností	Vysoká	**8.2**
10.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**7.8**
11.	Aruba Networks ClearPass Policy Manager - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
12.	stb_vorbis - bezpečnostná zraniteľnosť	Vysoká	**7.3**
13.	HPE OneView - bezpečnostná zraniteľnosť	Vysoká	**7.2**
14.	Dell Unity, Unity VSA a Unity XT - viacero bezpečnostných zraniteľností	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:
01794/2022/SK-CERT-1387

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

Identifikátor

SICK Flexi Soft Gateway - kritická bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu SICK Flexi Soft Gateway.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

24.10.2023

CVE

CVE-2023-5246

Zasiahnuté systémy

SICK Flexi Soft Gateway vo všetkých verziách

Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Odporúčame systémy zabezpečiť podľa odporúčaní výrobcu, ktoré môžete nájsť online na:
https://www.boschrexroth.com/en/us/media-details/c21792b6-da0b-4aaf-95ea-aaacfeb73139.
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.
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.

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-164691.html

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

Identifikátor

Google 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

24.10.2023

CVE

CVE-2023-23583, CVE-2023-40283, CVE-2023-42753, CVE-2023-5218

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 114.0.5735.338

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2023/10/long-term-support-channel-update-for_24.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/269417

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 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

24.10.2023

CVE

CVE-2023-5721, CVE-2023-5722, CVE-2023-5723, CVE-2023-5724, CVE-2023-5725, CVE-2023-5726, CVE-2023-5727, CVE-2023-5728, CVE-2023-5729, CVE-2023-5730, CVE-2023-5731, CVE-2023-5732, CVE-2023-5758

Zasiahnuté systémy

Firefox ESR vo verzii staršej ako 115.4
Thunderbird vo verzii staršej ako 115.4.1
Firefox for iOS vo verzii staršej ako 119
Firefox vo verzii staršej ako 119

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/269414
https://www.mozilla.org/en-US/security/advisories/mfsa2023-46/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-47/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-45/

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

Identifikátor

Roundcube - bezpečnostná zraniteľnosť

Popis

Vývojári webmailu Roundcube vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej e-mailovej správy vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

25.10.2023

CVE

CVE-2023-5631

Zasiahnuté systémy

Roundcube vo verzii staršej ako 1.4.15, 1.5.5, a 1.6.4

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://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/
https://nvd.nist.gov/vuln/detail/CVE-2023-5631
https://roundcube.net/news/2023/10/16/security-update-1.6.4-released
https://github.com/roundcube/roundcubemail/issues/9168

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

Identifikátor

Kubernetes ingress-nginx - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Kubernetes ingress-nginx. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.10.2023

CVE

CVE-2022-4886, CVE-2023-5043, CVE-2023-5044

Zasiahnuté systémy

Kubernetes ingress-nginx vo verzii staršej ako v1.9.0 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://seclists.org/oss-sec/2023/q4/185
https://exchange.xforce.ibmcloud.com/vulnerabilities/269578
https://exchange.xforce.ibmcloud.com/vulnerabilities/269574
https://exchange.xforce.ibmcloud.com/vulnerabilities/269570
https://github.com/kubernetes/ingress-nginx/issues/10570

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

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Safari, 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

25.10.2023

CVE

CVE-2023-30774, CVE-2023-32359, CVE-2023-32434, CVE-2023-38403, CVE-2023-40401, CVE-2023-40404, CVE-2023-40405, CVE-2023-40408, CVE-2023-40413, CVE-2023-40416, CVE-2023-40421, CVE-2023-40423, CVE-2023-40425, CVE-2023-40444, CVE-2023-40445, CVE-2023-40447, CVE-2023-40449, CVE-2023-41072, CVE-2023-41077, CVE-2023-41254, CVE-2023-41975, CVE-2023-41976, CVE-2023-41977, CVE-2023-41982, CVE-2023-41983, CVE-2023-41988, CVE-2023-41989, CVE-2023-41997, CVE-2023-42438, CVE-2023-42841, CVE-2023-42842, CVE-2023-42844, CVE-2023-42845, CVE-2023-42846, CVE-2023-42847, CVE-2023-42849, CVE-2023-42850, CVE-2023-42852, CVE-2023-42854, CVE-2023-42856, CVE-2023-42857, CVE-2023-42861, CVE-2023-4733, CVE-2023-4734, CVE-2023-4735, CVE-2023-4736, CVE-2023-4738, CVE-2023-4750, CVE-2023-4751, CVE-2023-4752, CVE-2023-4781

Zasiahnuté systémy

iOS vo verzii staršej ako 17.1
iPadOS vo verzii staršej ako 17.1
Safari vo verzii staršej ako 17.1
watchOS vo verzii staršej ako 10.1
tvOS vo verzii staršej ako 17.1
macOS Monterey vo verzii staršej ako 12.7.1
macOS Ventura vo verzii staršej ako 13.6.1
macOS Sonoma vo verzii staršej ako 14.1
iOS vo verzii staršej ako 15.8
iPadOS vo verzii staršej ako 15.8
iOS vo verzii staršej ako 16.7.2
iPadOS vo verzii staršej ako 16.7.2

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. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje
https://support.apple.com/en-us/HT213982 https://support.apple.com/en-us/HT213986 https://support.apple.com/en-us/HT213988 https://support.apple.com/en-us/HT213987 https://support.apple.com/en-us/HT213983 https://support.apple.com/en-us/HT213985 https://support.apple.com/en-us/HT213984 https://support.apple.com/en-us/HT213990 https://support.apple.com/en-us/HT213981 https://exchange.xforce.ibmcloud.com/vulnerabilities/269521

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

Identifikátor

Tenda W18E - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o kritickej zraniteľnosti produktu Tenda W18E.
Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.10.2023

CVE

CVE-2023-46369, CVE-2023-46370

Zasiahnuté systémy

Tenda W18E vo verzii firmvéru staršej ako 16.01.0.8(1576) (vrátane)

Následky

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

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
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://exchange.xforce.ibmcloud.com/vulnerabilities/269617
https://exchange.xforce.ibmcloud.com/vulnerabilities/269618

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

Identifikátor

Home Assistant Companion App for iOS - bezpečnostná zraniteľnosť

Popis

Vývojári aplikácie Home Assistant Companion vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

19.10.2023

CVE

CVE-2023-44385

Zasiahnuté systémy

Home Assistant Companion App pre iOS vo verzii staršej ako 2023.7

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/269286
https://nvd.nist.gov/vuln/detail/CVE-2023-44385

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

Identifikátor

IBM Security Verify Governance - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Verify Governance, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.10.2023

CVE

CVE-2010-2245, CVE-2016-0701, CVE-2016-10540, CVE-2017-16137, CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2017-5249, CVE-2018-0732, CVE-2018-0734, CVE-2018-0737, CVE-2018-0739, CVE-2018-1058, CVE-2018-16492, CVE-2018-3739, CVE-2018-5407, CVE-2019-10196, CVE-2019-1547, CVE-2019-1551, CVE-2019-1552, CVE-2019-1559, CVE-2019-1563, CVE-2019-9193, CVE-2020-15133, CVE-2020-1971, CVE-2020-35490, CVE-2020-35491, CVE-2020-7662, CVE-2020-7774, CVE-2021-23343, CVE-2021-3393, CVE-2021-3918, CVE-2021-4160, CVE-2022-21704, CVE-2022-22466, CVE-2022-40609, CVE-2023-33837, CVE-2023-33839, CVE-2023-33840

Zasiahnuté systémy

IBM Security Verify Governance vo verzii staršej ako 10.0

Následky

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

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.ibm.com/support/pages/node/7057377
https://exchange.xforce.ibmcloud.com/vulnerabilities/256036

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, 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 znepristupnenie služby.

Dátum prvého zverejnenia varovania

23.10.2023

CVE

CVE-2023-5633

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 6.6-rc6

Následky

Eskalácia privilégií
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://exchange.xforce.ibmcloud.com/vulnerabilities/269432
https://bugzilla.redhat.com/show_bug.cgi?id=2245663

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

Identifikátor

Aruba Networks ClearPass Policy Manager - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Aruba Networks vydala bezpečnostné aktualizácie na produkt ClearPass Policy Manager, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.10.2023

CVE

CVE-2023-43506, CVE-2023-43507, CVE-2023-43508, CVE-2023-43509, CVE-2023-43510

Zasiahnuté systémy

ClearPass Policy Manager 6.11.x vo verzii staršej ako 6.11.5
ClearPass Policy Manager 6.10.x ClearPass vo verzii staršej ako 6.10.8 Hotfix Q4 2023
ClearPass Policy Manager 6.9.x: ClearPass vo verzii staršej ako 6.9.13 Hotfix Q4 2023

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://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-016.txt
https://exchange.xforce.ibmcloud.com/vulnerabilities/269491

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

Identifikátor

stb_vorbis - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti knižnice stb_vorbis.
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

19.10.2023

CVE

CVE-2023-45681

Zasiahnuté systémy

stb_image vo verzii staršej ako v2.28
stb_vorbis vo verzii staršej ako v1.22

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://securitylab.github.com/advisories/GHSL-2023-145_GHSL-2023-151_stb_image_h/
https://exchange.xforce.ibmcloud.com/vulnerabilities/269216

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HPE OneView - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt OneView, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.10.2023

CVE

CVE-2023-30912

Zasiahnuté systémy

HPE OneView vo verzii staršej ako 8.60.00

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04548en_us

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

Identifikátor

Dell Unity, Unity VSA a Unity XT - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty Unity, Unity VSA a Unity XT, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.10.2023

CVE

CVE-2015-20107, CVE-2015-8985, CVE-2018-18074, CVE-2018-19416, CVE-2018-19517, CVE-2018-20060, CVE-2018-8956, CVE-2019-11236, CVE-2019-11324, CVE-2019-14250, CVE-2019-15847, CVE-2019-16167, CVE-2019-20454, CVE-2019-20838, CVE-2019-5021, CVE-2019-9740, CVE-2020-10683, CVE-2020-11868, CVE-2020-12049, CVE-2020-12825, CVE-2020-13817, CVE-2020-13844, CVE-2020-13956, CVE-2020-14155, CVE-2020-15025, CVE-2020-16590, CVE-2020-16591, CVE-2020-16592, CVE-2020-16593, CVE-2020-16598, CVE-2020-16599, CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687, CVE-2020-26116, CVE-2020-35448, CVE-2020-35493, CVE-2020-35496, CVE-2020-35507, CVE-2020-35512, CVE-2021-20197, CVE-2021-20284, CVE-2021-20294, CVE-2021-21342, CVE-2021-23214, CVE-2021-23222, CVE-2021-25220, CVE-2021-26720, CVE-2021-33560, CVE-2021-3448, CVE-2021-3468, CVE-2021-3487, CVE-2021-3572, CVE-2021-3580, CVE-2021-3672, CVE-2021-37600, CVE-2021-38185, CVE-2021-3973, CVE-2021-3999, CVE-2021-40330, CVE-2021-4149, CVE-2021-41617, CVE-2021-4197, CVE-2021-4202, CVE-2021-43565, CVE-2021-44879, CVE-2022-0001, CVE-2022-0002, CVE-2022-0322, CVE-2022-0330, CVE-2022-0435, CVE-2022-0487, CVE-2022-0492, CVE-2022-0561, CVE-2022-0562, CVE-2022-0617, CVE-2022-0644, CVE-2022-0778, CVE-2022-0865, CVE-2022-0891, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924, CVE-2022-0934, CVE-2022-1056, CVE-2022-1097, CVE-2022-1271, CVE-2022-1292, CVE-2022-1304, CVE-2022-1587, CVE-2022-2068, CVE-2022-2097, CVE-2022-21151, CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21476, CVE-2022-21496, CVE-2022-23181, CVE-2022-23218, CVE-2022-23219, CVE-2022-23308, CVE-2022-23648, CVE-2022-24407, CVE-2022-24448, CVE-2022-24765, CVE-2022-24769, CVE-2022-24959, CVE-2022-25762, CVE-2022-26373, CVE-2022-26377, CVE-2022-27191, CVE-2022-28614, CVE-2022-28615, CVE-2022-29162, CVE-2022-29187, CVE-2022-29404, CVE-2022-30522, CVE-2022-30556, CVE-2022-31030, CVE-2022-31676, CVE-2022-31741, CVE-2022-31813, CVE-2022-41946, CVE-2023-43065, CVE-2023-43066, CVE-2023-43067, CVE-2023-43074

Zasiahnuté systémy

Dell Unity Operating Environment (OE) vo verzii staršej ako 5.3.0.0.5.120
Dell Unity VSA Operating Environment (OE) vo verzii staršej ako 5.3.0.0.5.120
Dell Unity XT Operating Environment (OE) vo verzii staršej ako 5.3.0.0.5.120

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities https://exchange.xforce.ibmcloud.com/vulnerabilities/269366