BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 03. 2022 - 15. 03. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apple iOS a iPadOS produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	UltraVNC server - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	HP UEFI Firmware - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	AVEVA System Platform - bezpečnostná zraniteľnosť	Vysoká	**8.1**
05.	Linux Kernel - dve bezpečnostné zraniteľnosi	Vysoká	**7.8**
06.	Istio produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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

Identifikátor

Apple iOS a iPadOS produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na produkty iOS a iPadOS, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvoreného súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.03.2022

CVE

CVE-2021-36976, CVE-2022-22596, CVE-2022-22598, CVE-2022-22599, CVE-2022-22600, CVE-2022-22609, CVE-2022-22610, CVE-2022-22611, CVE-2022-22612, CVE-2022-22613, CVE-2022-22614, CVE-2022-22615, CVE-2022-22618, CVE-2022-22621, CVE-2022-22622, CVE-2022-22624, CVE-2022-22628, CVE-2022-22629, CVE-2022-22632, CVE-2022-22633, CVE-2022-22634, CVE-2022-22635, CVE-2022-22636, CVE-2022-22637, CVE-2022-22638, CVE-2022-22639, CVE-2022-22640, CVE-2022-22641, CVE-2022-22642, CVE-2022-22643, CVE-2022-22652, CVE-2022-22653, CVE-2022-22659, CVE-2022-22662, CVE-2022-22666, CVE-2022-22667, CVE-2022-22668, CVE-2022-22670, CVE-2022-22671

Zasiahnuté systémy

Apple iOS vo verzii staršej ako 15.4
Apple iPadOS vo verzii staršej ako 15.4

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.
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/HT213182
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22610
https://exchange.xforce.ibmcloud.com/vulnerabilities/221760

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

Identifikátor

UltraVNC server - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja UltraVNC server 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 eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.03.2022

CVE

CVE-2022-24750

Zasiahnuté systémy

UltraVNC server vo verzii staršej ako 1.3.8.1.

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Vývojári odporúčajú neinštalovať a nespúšťať server UltraVNC ako service ale vytvoriť naplánovanú úlohu na účte s nízkymi oprávneniami.
Po odstránení zraniteľností, ktoré mohli spôsobiť lokálne 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://github.com/ultravnc/UltraVNC/security/advisories/GHSA-3mvp-cp5x-vj5g
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24750
https://exchange.xforce.ibmcloud.com/vulnerabilities/221519

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

Identifikátor

HP UEFI Firmware - viacero bezpečnostných zraniteľností

Popis

Spoločnosť HP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

08.03.2022

CVE

CVE-2022-23924, CVE-2022-23925, CVE-2022-23926, CVE-2022-23927, CVE-2022-23928, CVE-2022-23929, CVE-2022-23930, CVE-2022-23931, CVE-2022-23932, CVE-2022-23933, CVE-2022-23934

Zasiahnuté systémy

HP UEFI Firmware
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://support.hp.com/us-en/document/ish_5817864-5817896-16

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 lokálne 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://binarly.io/posts/Repeatable_Firmware_Security_Failures_16_High_Impact_Vulnerabilities_Discovered_in_HP_Devices/index.html
https://www.bleepingcomputer.com/news/security/hp-patches-16-uefi-firmware-bugs-allowing-stealthy-malware-infections/
https://github.com/binarly-io/Vulnerability-REsearch/blob/main/Insyde/BRLY-2021-021.md
https://support.hp.com/us-en/document/ish_5817864-5817896-16

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

Identifikátor

AVEVA System Platform - bezpečnostná zraniteľnosť

Popis

Spoločnosť AVEVA vydala bezpečnostnú aktualizáciu na produkt System Platform, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.03.2022

CVE

CVE-2022-0835

Zasiahnuté systémy

AVEVA System Platform vo verzii staršej ako 2020 R2 SP1
AVEVA System Platform vo verzii staršej ako 2020 P01

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-067-02

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

Identifikátor

Linux Kernel - dve bezpečnostné zraniteľnosi

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti, z toho jednu známu ako "Dirty Pipe".
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.03.2022

CVE

CVE-2022-0847, CVE-2022-25636

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.16.11
Linux Kernel vo verzii staršej ako 5.15.25
Linux Kernel vo verzii staršej ako 5.10.102

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 lokálne 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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

http://www.dsl.sk/article.php?article=25925
https://thehackernews.com/2022/03/dirty-pipe-linux-flaw-affects-wide.html
https://thehackernews.com/2022/03/new-linux-bug-in-netfilter-firewall.html
https://seclists.org/oss-sec/2022/q1/170
https://dirtypipe.cm4all.com/
https://kernel.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847
https://exchange.xforce.ibmcloud.com/vulnerabilities/221112

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

Identifikátor

Istio produkt - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Istio vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.03.2022

CVE

CVE-2022-24726

Zasiahnuté systémy

Istio vo verzii staršej ako 1.13.2
Istio vo verzii staršej ako 1.12.5
Istio vo verzii staršej ako 1.11.8

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Vývojári ďalej odporúčajú zakázať prístup k overovaciemu webhooku, ktorý je vystavený verejnému internetu, alebo obmedziť množinu IP adries, ktoré ho môžu vyhľadávať, na množinu známych, dôveryhodných entít.

Zdroje

https://github.com/istio/istio/security/advisories/GHSA-8w5h-qr4r-2h6g
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24726
https://exchange.xforce.ibmcloud.com/vulnerabilities/221635

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-706