BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 01. 2022 - 01. 02. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Bosch produkty - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	F5 BIG-IP, BIG-IQ, a NGINX produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.7**
03.	Apple iOS a iPadOS produkty - bezpečnostná zraniteľnosť	Vysoká	**7.8**
04.	GE Gas Power ToolBoxST - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
05.	Synametrics SynaMan produkt - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	Microsoft Windows - bezpečnostná zraniteľnosť	Vysoká	**7.0**

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-665

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

Identifikátor

Bosch produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Bosch vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.01.2022

CVE

CVE-2021-23842, CVE-2021-23843

Zasiahnuté systémy

Bosch AMC2
Bosch AMS vo verzii staršej ako 4.0
Bosch APE vo verzii staršej ako 3.8.x (vrátane)
Bosch BIS vo verzii staršej ako 4.9.1

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-940448-bt.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

F5 BIG-IP, BIG-IQ, a NGINX produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie 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

19.01.2022

CVE

CVE-2022-23008, CVE-2022-23009, CVE-2022-23010, CVE-2022-23011, CVE-2022-23012, CVE-2022-23013, CVE-2022-23014, CVE-2022-23015, CVE-2022-23016, CVE-2022-23017, CVE-2022-23018, CVE-2022-23019, CVE-2022-23020, CVE-2022-23021, CVE-2022-23022, CVE-2022-23023, CVE-2022-23024, CVE-2022-23025, CVE-2022-23026, CVE-2022-23027, CVE-2022-23028, CVE-2022-23029, CVE-2022-23030, CVE-2022-23031, CVE-2022-23032

Zasiahnuté systémy

NGINX Controller API Management vo verzii staršej ako 3.19.1
BIG-IQ Centralized Management vo verzii staršej ako 8.1.0
BIG-IP vo verzii staršej ako 16.1.2
BIG-IP vo verzii staršej ako 15.1.4.1
BIG-IP vo verzii staršej ako 14.1.4.5

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.f5.com/csp/article/K40084114
https://support.f5.com/csp/article/K57735782
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/20/f5-releases-january-2022-quarterly-security-notification
https://www.securityweek.com/f5-patches-two-dozen-vulnerabilities-big-ip

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

Identifikátor

Apple iOS a iPadOS produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na produkty iOS a iPadOS, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.01.2022

CVE

CVE-2022-22587

Zasiahnuté systémy

Apple iPadOS vo verzii staršej ako 15.3
Apple iOS vo verzii staršej ako 15.3

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.
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).

Zdroje

https://thehackernews.com/2022/01/apple-releases-ios-and-ipados-updates.html
https://support.apple.com/en-us/HT213053
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22587
https://exchange.xforce.ibmcloud.com/vulnerabilities/218158

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

Identifikátor

GE Gas Power ToolBoxST - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť GE Gas Power vydala bezpečnostnú aktualizáciu na produkt ToolBoxST, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.01.2022

CVE

CVE-2018-16202, CVE-2021-44477

Zasiahnuté systémy

ToolBoxST OS vo verzii staršej ako 07.09.07C

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-025-01

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

Identifikátor

Synametrics SynaMan produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Synametrics vydala bezpečnostnú aktualizáciu na produkt SynaMan, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.01.2022

CVE

CVE-2022-22828

Zasiahnuté systémy

Synametrics SynaMan vo verzii staršej ako 5.0

Následky

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://github.com/videnlabs/CVE-2022-22828/
https://web.synametrics.com/SynamanVersionHistory.htm
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22828
https://exchange.xforce.ibmcloud.com/vulnerabilities/218336

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Windows - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj produkt Windows, ktorá opravuje bezpečnostnú zraniteľnosť.
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

29.01.2022

CVE

CVE-2022-21882

Zasiahnuté systémy

Windows 10 vo verzii staršej ako 20H2 pre 32-bit systémy
Windows 10 vo verzii staršej ako 20H2 pre x64-based systémy
Windows 10 vo verzii staršej ako 1909 pre ARM64-based systémy
Windows 10 vo verzii staršej ako 1909 pre x64-based systémy
Windows 10 vo verzii staršej ako 1909 pre 32-bit systémy
Windows 10 vo verzii staršej ako 21H2 pre x64-based systémy
Windows 10 vo verzii staršej ako 21H2 pre ARM64-based systémy
Windows 10 vo verzii staršej ako 21H2 pre 32-bit systémy
Windows 11 pre ARM64-based systémy
Windows 11 pre x64-based systémy
Windows Server, vo verzii staršej ako 20H2 (Server Core Installation)
Windows 10 vo verzii staršej ako 20H2 pre ARM64-based systémy
Windows Server 2022 Windows 10 vo verzii staršej ako 21H1 pre 32-bit systémy
Windows 10 vo verzii staršej ako 21H1 pre ARM64-based systémy
Windows 10 vo verzii staršej ako 21H1 pre x64-based systémy
Windows Server 2019 (Server Core installation)Windows Server 2019
Windows 10 vo verzii staršej ako 1809 pre ARM64-based systémy
Windows 10 vo verzii staršej ako 1809 pre x64-based systémy
Windows 10 vo verzii staršej ako 1809 pre 32-bit systémy

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

Zdroje
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882 https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/ https://twitter.com/wdormann/status/1487205136174878721 https://securityaffairs.co/wordpress/127377/hacking/cve-2022-21882-win-local-privilege-elevation.html