BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 01. 2023 - 10. 01. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Android OS - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Fortiguard - viacero bezpečnostných zraniteľností	Vysoká	**8.6**
03.	Lenovo ThinkPad X13s BIOS - viacero bezpečnostných zraniteľností	Vysoká	**8.4**
04.	Silverstripe CMS - bezpečnostná zraniteľnosť	Vysoká	**7.5**
05.	Garmin Connect - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	Apache Tomcat - bezpečnostná zraniteľnosť	Vysoká	**7.5**
07.	NETGEAR - bezpečnostná zraniteľnosť	Vysoká	**7.4**
08.	b2evolution CMS - bezpečnostná zraniteľnosť	Vysoká	**7.2**

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-984

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

Identifikátor

Google Android OS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom znovupoužitia uvoľnenej pamäte vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.01.2023

CVE

CVE-2021-35097, CVE-2021-35113, CVE-2021-35134, CVE-2022-20235, CVE-2022-20456, CVE-2022-20461, CVE-2022-20489, CVE-2022-20490, CVE-2022-20492, CVE-2022-20493, CVE-2022-20494, CVE-2022-22088, CVE-2022-23960, CVE-2022-25725, CVE-2022-25746, CVE-2022-2959, CVE-2022-32635, CVE-2022-32636, CVE-2022-32637, CVE-2022-33252, CVE-2022-33253, CVE-2022-33255, CVE-2022-33266, CVE-2022-33274, CVE-2022-33276, CVE-2022-33283, CVE-2022-33284, CVE-2022-33285, CVE-2022-33286, CVE-2022-41674, CVE-2022-42719, CVE-2022-42720, CVE-2022-42721, CVE-2022-44425, CVE-2022-44426, CVE-2022-44427, CVE-2022-44428, CVE-2022-44429, CVE-2022-44430, CVE-2022-44431, CVE-2022-44432, CVE-2022-44434, CVE-2022-44435, CVE-2022-44436, CVE-2022-44437, CVE-2022-44438, CVE-2023-20904, CVE-2023-20905, CVE-2023-20908, CVE-2023-20912, CVE-2023-20913, CVE-2023-20915, CVE-2023-20916, CVE-2023-20918, CVE-2023-20919, CVE-2023-20920, CVE-2023-20921, CVE-2023-20922, CVE-2023-20928

Zasiahnuté systémy

Android OS patch levels prior to 2023-01-05

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://source.android.com/docs/security/bulletin/2023-01-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2023-001
https://nvd.nist.gov/vuln/detail/CVE-2022-42719

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

Identifikátor

Fortiguard - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na produkty zo súpravy Fortiguard, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.01.2023

CVE

CVE-2022-35845, CVE-2022-39947, CVE-2022-41336, CVE-2022-45857

Zasiahnuté systémy

FortiADC vo verzii staršej ako 6.2.4 a 7.0.2
FortiTester vo verzii staršej ako 3.9.2, 4.2.1, 7.1.1, a 7.2.0.
FortiManager vo verzii staršej ako 6.2.9, 6.4.8 a 7.0.2
FortiPortal vo verzii staršej ako 6.0.12
FortiWeb vo verzii staršej ako 7.2.0 a 7.0.3

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.fortiguard.com/psirt/FG-IR-22-061
https://www.securityweek.com/high-severity-command-injection-flaws-found-fortinets-fortitester-fortiadc

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Lenovo ThinkPad X13s BIOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu BIOS na svoje portfólio notebookov rady ThinkPad X13s, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom pretečenia zásobníka spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.01.2023

CVE

CVE-2022-40516, CVE-2022-40517, CVE-2022-40518, CVE-2022-40519, CVE-2022-40520, CVE-2022-4432, CVE-2022-4433, CVE-2022-4434, CVE-2022-4435

Zasiahnuté systémy

ThinkPad X13s BIOS vo verzii staršej ako 1.47 (N3HET75W)

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie.
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.lenovo.com/us/en/product_security/LEN-103709
https://nvd.nist.gov/vuln/detail/CVE-2022-40516

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

Identifikátor

Silverstripe CMS - bezpečnostná zraniteľnosť

Popis

Vývojári redakčného systému Silverstripe 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 požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

29.12.2022

CVE

CVE-2022-42949

Zasiahnuté systémy

silverstripe/subsites vo verzii staršej ako 2.7.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie nie sú založené na redakčnom systéme Silverstripe v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://www.silverstripe.org/download/security-releases/cve-2022-42949
https://exchange.xforce.ibmcloud.com/vulnerabilities/243572

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

Identifikátor

Garmin Connect - bezpečnostná zraniteľnosť

Popis

Spoločnosť Garmin vydala bezpečnostnú aktualizáciu na svoju aplikáciu Garmin Connect, 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

31.12.2022

CVE

CVE-2022-46081

Zasiahnuté systémy

Garmin Connect vo verzii staršej ako 4.62

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://exchange.xforce.ibmcloud.com/vulnerabilities/243705

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

Identifikátor

Apache Tomcat - bezpečnostná zraniteľnosť

Popis

Vývojári servletu Apache Tomcat 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 požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

03.01.2022

CVE

CVE-2022-45143

Zasiahnuté systémy

Apache Tomcat vo verzii staršej ako 8.5.84, 9.0.69 a 10.1.2

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2023/q1/2
https://exchange.xforce.ibmcloud.com/vulnerabilities/243565

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

Identifikátor

NETGEAR - bezpečnostná zraniteľnosť

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoje portfólio routerov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.12.2022

CVE

CVE-2022-48196

Zasiahnuté systémy

RAX40 s firmvérom vo verzii staršej ako 1.0.2.60
RAX35 s firmvérom vo verzii staršej ako 1.0.2.60
R6400v2 s firmvérom vo verzii staršej ako 1.0.4.122
R6700v3 s firmvérom vo verzii staršej ako 1.0.4.122
R6900P s firmvérom vo verzii staršej ako 1.3.3.152
R7000P s firmvérom vo verzii staršej ako 1.3.3.152
R7000 s firmvérom vo verzii staršej ako 1.0.11.136
R7960P s firmvérom vo verzii staršej ako 1.4.4.94
R8000P s firmvérom vo verzii staršej ako 1.4.4.94

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://kb.netgear.com/000065495/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2019-0208
https://exchange.xforce.ibmcloud.com/vulnerabilities/243425

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

Identifikátor

b2evolution CMS - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti redakčného systému b2evolution. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.12.2022

CVE

CVE-2022-44036

Zasiahnuté systémy

b2evolution vo verzii staršej ako 7.2.5 (vrátane)

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie nie sú založené na redakčnom systéme b2evolution v zraniteľnej verzii. V prípade, že áno, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje

https://github.com/b2evolution/b2evolution/issues/121
https://exchange.xforce.ibmcloud.com/vulnerabilities/243566