BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 12. 2023 - 02. 01. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-1453

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

Identifikátor

Apache OpenOffice - bezpečnostná zraniteľnosť

Popis

Vývojári balíka Apache OpenOffice 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 vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľností vyžaduje interakciu používateľov.

Dátum prvého zverejnenia varovania

27.12.2023

CVE

CVE-2023-47804

Zasiahnuté systémy

Apache OpenOffice vo verzii staršej ako 4.1.15 (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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://seclists.org/oss-sec/2023/q4/343
https://exchange.xforce.ibmcloud.com/vulnerabilities/276126

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Google 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

02.01.2024

CVE

CVE-2024-0222, CVE-2024-0223, CVE-2024-0224, CVE-2024-0225

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 120.0.6099.199
Chrome pre Windows vo verzii staršej ako 120.0.6099.199/200
Chrome pre Android vo verzii staršej ako 120.0.6099.193

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/2024/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2024/01/chrome-for-android-update.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/278410

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

Identifikátor

Google Android - 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 útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom znovupoužitia uvoľnenej pamäte vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.01.2024

CVE

CVE-2022-33275, CVE-2023-21165, CVE-2023-21245, CVE-2023-21651, CVE-2023-28544, CVE-2023-28548, CVE-2023-28557, CVE-2023-28558, CVE-2023-28559, CVE-2023-28560, CVE-2023-28564, CVE-2023-28565, CVE-2023-28567, CVE-2023-32872, CVE-2023-32874, CVE-2023-33014, CVE-2023-33025, CVE-2023-33030, CVE-2023-33032, CVE-2023-33033, CVE-2023-33036, CVE-2023-33037, CVE-2023-33040, CVE-2023-33043, CVE-2023-33044, CVE-2023-33062, CVE-2023-33094, CVE-2023-33108, CVE-2023-33109, CVE-2023-33110, CVE-2023-33112, CVE-2023-33113, CVE-2023-33114, CVE-2023-33117, CVE-2023-33120, CVE-2023-40085, CVE-2023-4295, CVE-2023-43511, CVE-2023-43514, CVE-2023-48340, CVE-2023-48341, CVE-2023-48342, CVE-2023-48343, CVE-2023-48344, CVE-2023-48348, CVE-2023-48349, CVE-2023-48350, CVE-2023-48351, CVE-2023-48352, CVE-2023-5427, CVE-2024-0015, CVE-2024-0016, CVE-2024-0017, CVE-2024-0018, CVE-2024-0019, CVE-2024-0020, CVE-2024-0021, CVE-2024-0023

Zasiahnuté systémy

Google Android s bezpečnostnou aktualizáciou úrovne staršej ako 2024-01-05

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/2024-01-01
https://nvd.nist.gov/vuln/detail/CVE-2023-40088

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

Identifikátor

OnCell G3150A-LTE Series - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Moxa vydala bezpečnostnú aktualizáciu na svoj produkt OnCell série G3150A-LTE, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať MITM (Man In The Middle) útok a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

29.12.2023

CVE

CVE-2004-2761, CVE-2013-2566, CVE-2016-2183, CVE-2023-6093, CVE-2023-6094

Zasiahnuté systémy

OnCell G3150A-LTE Series vo verzii staršej ako 1.3

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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.moxa.com/en/support/product-support/security-advisory/oncell-g3150a-lte-series-multiple-web-application-vulnerabilities-and-security-enhancement

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

Identifikátor

HPE Unified OSS Console - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt Unified OSS Console, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

02.01.2024

CVE

CVE-2023-31582, CVE-2023-42795, CVE-2023-44487, CVE-2023-45648

Zasiahnuté systémy

HPE Unified OSS Console (UOC) vo verzii staršej ako v3.1.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04570en_us