# BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 04. 2022 - 13. 04. 2022

## OBSAH BEZPEČNOSTNÉHO BULLETINU

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

## Identifikátor

ManageEngine ADSelfService Plus - bezpečnostná zraniteľnosť

## Popis

Vývojári nástroja ManageEngine ADSelfService Plus vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

09.04.2022

## CVE

CVE-2022-28810

## Zasiahnuté systémy

ManageEngine ADSelfService Plus vo verzii staršej ako Build 6122

## 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.manageengine.com/products/self-service-password/kb/cve-2022-28810.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28810
https://exchange.xforce.ibmcloud.com/vulnerabilities/223803

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

## Identifikátor

Google Android - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na produkt Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.04.2022

## CVE

CVE-2021-0694, CVE-2021-0707, CVE-2021-25477, CVE-2021-30281, CVE-2021-30334, CVE-2021-30338, CVE-2021-30339, CVE-2021-30340, CVE-2021-30341, CVE-2021-30342, CVE-2021-30343, CVE-2021-30344, CVE-2021-30345, CVE-2021-30346, CVE-2021-30347, CVE-2021-30349, CVE-2021-30350, CVE-2021-35070, CVE-2021-35081, CVE-2021-35091, CVE-2021-35095, CVE-2021-35100, CVE-2021-35104, CVE-2021-35112, CVE-2021-35123, CVE-2021-35130, CVE-2021-39794, CVE-2021-39795, CVE-2021-39796, CVE-2021-39797, CVE-2021-39798, CVE-2021-39799, CVE-2021-39800, CVE-2021-39801, CVE-2021-39802, CVE-2021-39803, CVE-2021-39804, CVE-2021-39805, CVE-2021-39807, CVE-2021-39808, CVE-2021-39809, CVE-2022-20081

## Zasiahnuté systémy

Google Android vo verzii staršej ako 2021-04-05

## Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby
Eskalácia privilégií

## 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://source.android.com/security/bulletin/2022-04-01
https://www.securityweek.com/44-vulnerabilities-patched-android-april-2022-security-updates

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

## Identifikátor

SiteGround Security plugin pre WordPress - bezpečnostná zraniteľnosť

## Popis

Vývojári SiteGround Security pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

08.04.2022

## CVE

CVE-2022-0993

## Zasiahnuté systémy

WordPress SiteGround Security plugin pre WordPress vo verzii staršej ako 1.2.6

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK 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 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://wordpress.org/plugins/sg-security/
https://packetstormsecurity.com/files/166642
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0993
https://exchange.xforce.ibmcloud.com/vulnerabilities/223808

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

## Identifikátor

ABB Symphony Plus SPIET800 a PNI800 produkt - viacero bezpečnostných zraniteľností

## Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na produkty Symphony Plus SPIET800 a PNI800, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

08.04.2022

## CVE

CVE-2021-22285, CVE-2021-22286, CVE-2021-22288

## Zasiahnuté systémy

SPIET800 s firmware vo verzii staršej ako A_C
PNI800 s firmware vo verzii staršej ako B_0

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

## Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-097-02

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

## Identifikátor

Citrix Hypervisor a XenServer - bezpečnostná zraniteľnosť

## Popis

Spoločnosť Citrix vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.04.2022

## CVE

CVE-2022-26357

## Zasiahnuté systémy

Citrix Hypervisor vo verzii staršej ako 8.2 CU1 LTSR: CTX376976
Citrix Hypervisor vo verzii staršej ako 8.2: CTX376939
Citrix XenServer vo verzii staršej ako 7.1 CU2 LTSR: CTX376940

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://support.citrix.com/article/CTX390511
https://support.citrix.com/article/CTX376976
https://support.citrix.com/article/CTX376939
https://support.citrix.com/article/CTX376940

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

## Identifikátor

Node.js directus modul - bezpečnostná zraniteľnosť

## Popis

Vývojári modulu directus pre Node.js vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

## Dátum prvého zverejnenia varovania

07.04.2022

## CVE

CVE-2022-26969

## Zasiahnuté systémy

Node.js directus vo verzii staršej ako 9.7.0

## Následky

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

## Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK 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 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://security.snyk.io/vuln/SNYK-JS-DIRECTUS-2441822
https://github.com/directus/directus/pull/12022
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26969
https://exchange.xforce.ibmcloud.com/vulnerabilities/223871

**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-732