BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 07. 2022 - 12. 07. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	SAP 3D Visual Enterprise Viewer - bezpčnostná zraniteľnosť	Vysoká	**8.8**
02.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**8.2**
03.	Kubernetes SIGs AWS IAM Authenticator - bezpečnostná zraniteľnosť	Vysoká	**8.1**
04.	Fortinet produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.0**
05.	Google Android - viacero bezpečnostných zraniteľností	Vysoká	**7.3**
06.	Schneider Electric Acti9 PowerTag Link C - bezpečnostná zraniteľnosť	Stredná	**6.8**

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-824

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

Identifikátor

SAP 3D Visual Enterprise Viewer - bezpčnostná zraniteľnosť

Popis

Spoločnosť SAP vydala bezpečnostnú aktualizáciu na svoj produkt 3D Visual Enterprise Viewer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených HDR súborov vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.07.2022

CVE

CVE-2022-32242

Zasiahnuté systémy

SAP 3D Visual Enterprise Viewer vo verzii staršej ako 9.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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.zerodayinitiative.com/advisories/ZDI-22-956/
https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť nachádzajúca sa v LightNVM subsystéme spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2022

CVE

-

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.19-rc6

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.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-22-961/
https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/drivers/lightnvm/Kconfig?h=v5.10.114&id=549209caabc89f2877ad5f62d11fca5c052e0e8

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

Identifikátor

Kubernetes SIGs AWS IAM Authenticator - bezpečnostná zraniteľnosť

Popis

Vývojári Kubernetes SIGs vydali bezpečnostnú aktualizáciu na svoj produkt AWS IAM Authenticator, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených požiadaviek eskalovať svoje privilégiá a následne spôsobiť narušenie dôvernosti a integrity systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-2385

Zasiahnuté systémy

AWS IAM Authenticator vo verzii staršej ako 0.5.9

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti a integrity systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/230847
https://github.com/kubernetes-sigs/aws-iam-authenticator/issues/472

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Fortinet produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na svoje produkty FortiADC, FortiAnalyzer, FortiClientWindows, FortiDeJuneentral, FortiDeceptor, FortiEDR, FortiManager, FortiNAC, FortiOS, FortiProxy, FortiRecorder, FortiSwitch, FortiVoiceEnterprise a JuneFortiManager, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.07.2022

CVE

CVE-2021-4103, CVE-2021-42755, CVE-2021-43072, CVE-2021-44170, CVE-2022-2274, CVE-2022-23438, CVE-2022-26117, CVE-2022-26118, CVE-2022-26120, CVE-2022-27483, CVE-2022-29057, CVE-2022-30302

Zasiahnuté systémy
FortiADC vo verzii staršej ako 6.2.3
FortiADC vo verzii staršej ako 7.0.2
FortiAnalyzer vo verzii staršej ako 6.4.8
FortiAnalyzer vo verzii staršej ako 7.0.3
FortiAnalyzer vo verzii staršej ako 7.0.4
FortiAnalyzer vo verzii staršej ako 7.2.0
FortiClientWindows vo verzii staršej ako 6.4.7
FortiClientWindows vo verzii staršej ako 7.0.3
FortiDeJuneentral Manager vo verzii staršej ako 5.2.0
FortiDeceptor vo verzii staršej ako 4.0.2
FortiDeceptor vo verzii staršej ako 4.1.0
FortiEDR Central Manager vo verzii staršej ako 5.0.3 Patch 7
FortiManager vo verzii staršej ako 6.4.8
FortiManager vo verzii staršej ako 7.0.4
FortiManager vo verzii staršej ako 7.2.0
FortiNAC vo verzii staršej ako 9.1.6
FortiNAC vo verzii staršej ako 9.2.4
FortiOS vo verzii staršej ako 6.2.11
FortiOS vo verzii staršej ako 6.2.11
FortiOS vo verzii staršej ako 6.4.9
FortiOS vo verzii staršej ako 7.0.4
FortiOS vo verzii staršej ako 7.0.6
FortiOS vo verzii staršej ako 7.2.0
FortiProxy verJune vo verzii staršej ako 6.4.9
FortiProxy vo verzii staršej ako 2.0.7
FortiProxy vo verzii staršej ako 2.0.9
FortiProxy vo verzii staršej ako 7.0.1
FortiProxy vo verzii staršej ako 7.0.4
FortiRecorder vo verzii staršej ako 6.0.11
FortiRecorder vo verzii staršej ako 6.4.3
FortiSwitch vo verzii staršej ako 6.4.10
FortiSwitch vo verzii staršej ako 7.0.3
FortiSwitch vo verzii staršej ako 7.2.0
FortiVoiceEnterprise vo verzii staršej ako 6.0.11
FortiVoiceEnterprise vo verzii staršej ako 6.4.4
JuneFortiManager vo verzii staršej ako 7.0.3

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

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
www.securitynewspaper.com/2022/07/07/11-important-vulnerabilities-in-fortinet-products-fortios-fortianalyzer-fortiadc-fortimanager-fortiproxy-forticlient-fortideceptor-fortiswitch-fortirecoder-fortivoiceenterprise/
https://www.fortiguard.com/psirt/FG-IR-22-051
https://www.fortiguard.com/psirt/FG-IR-22-049
https://www.fortiguard.com/psirt/FG-IR-21-206
https://www.fortiguard.com/psirt/FG-IR-21-190
https://www.fortiguard.com/psirt/FG-IR-21-213
https://www.fortiguard.com/psirt/FG-IR-22-077
https://www.fortiguard.com/psirt/FG-IR-21-056
https://www.fortiguard.com/psirt/FG-IR-22-058
https://www.fortiguard.com/psirt/FG-IR-21-179
https://www.fortiguard.com/psirt/FG-IR-21-057
https://www.fortiguard.com/psirt/FG-IR-21-155

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
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 vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.07.2022

CVE

CVE-2021-0981, CVE-2022-20221, CVE-2022-20222, CVE-2022-20223, CVE-2022-20224, CVE-2022-20225, CVE-2022-20226, CVE-2022-20229, CVE-2022-20230

Zasiahnuté systémy

Google Android s bezpečnostnou aktualizáciou spred 5. Júla 2022

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2022-088
https://source.android.com/security/bulletin/2022-07-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schneider Electric Acti9 PowerTag Link C - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Acti9 PowerTag Link C, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi s fyzickým prístupom k systému eskalovať svoje privilégiá a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-34754

Zasiahnuté systémy

Acti9 PowerTag Link C vo verzii firmvéru staršej ako V2.14.0

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

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

Zdroje

https://www.se.com/ww/en/download/document/SEVD-2022-193-03/