BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 08. 2022 - 09. 08. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Ecwid Ecommerce Shopping Cart plugin - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Google Android - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Nuki Smart Lock - viacero bezpečnostných zraniteľností	Vysoká	**8.0**
04.	nVidia - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
05.	Kaspersky VPN Secure Connection - bezpečnostná zraniteľnosť	Vysoká	**7.8**
06.	Apache Hadoop - bezpečnostná zraniteľnosť	Vysoká	**7.8**
07.	Autodesk - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
08.	F5 BIG-IP - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
09.	GitLab - viacero bezpečnostných zraniteľností	Stredná	**6.4**

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-850

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

Identifikátor

Ecwid Ecommerce Shopping Cart plugin - bezpečnostná zraniteľnosť

Popis

Spoločnosť Ecwid vydala bezpečnostnú aktualizáciu na svoj WordPress plugin Ecommerce Shopping Cart, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.08.2022

CVE

CVE-2022-2432

Zasiahnuté systémy

Ecwid Ecommerce Shopping Cart plugin pre WordPress vo verzii staršej ako 4.4.3 (vrátane)
Ecwid Ecommerce Shopping Cart plugin pre WordPress staršej ako 6.10.24

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

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.
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 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://patchstack.com/database/vulnerability/ecwid-shopping-cart/wordpress-ecwid-ecommerce-shopping-cart-plugin-6-10-23-cross-site-request-forgery-csrf-vulnerability-leading-to-settings-options-update

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 open source operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky cez Bluetooth vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.08.2022

CVE

CVE-2021-0698, CVE-2021-0887, CVE-2021-0891, CVE-2021-0946, CVE-2021-0947, CVE-2021-30259, CVE-2021-39696, CVE-2021-39815, CVE-2022-1786, CVE-2022-20082, CVE-2022-20122, CVE-2022-20239, CVE-2022-20344, CVE-2022-20345, CVE-2022-20346, CVE-2022-20347, CVE-2022-20348, CVE-2022-20349, CVE-2022-20350, CVE-2022-20352, CVE-2022-20353, CVE-2022-20354, CVE-2022-20355, CVE-2022-20356, CVE-2022-20357, CVE-2022-20358, CVE-2022-20360, CVE-2022-20361, CVE-2022-22059, CVE-2022-22061, CVE-2022-22062, CVE-2022-22067, CVE-2022-22069, CVE-2022-22070, CVE-2022-22080, CVE-2022-25668

Zasiahnuté systémy

Google Android s bezpečnostnou aktualizáciou spred 1. Augusta 2022

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/security/bulletin/2022-08-01
https://www.securityweek.com/google-patches-critical-android-flaw-allowing-remote-code-execution-bluetooth
https://www.redpacketsecurity.com/google-android-code-execution-cve-2022-20345/

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

Identifikátor

Nuki Smart Lock - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Nuki vydala bezpečnostné aktualizácie na produkty Nuki Smart Lock, Bridge, Keypad, Fob a Smart Lock application, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.07.2022

CVE

CVE-2022-32502, CVE-2022-32503, CVE-2022-32504, CVE-2022-32505, CVE-2022-32506, CVE-2022-32507, CVE-2022-32508, CVE-2022-32509, CVE-2022-32510

Zasiahnuté systémy

Nuki Smart Lock 3.0 vo verzii staršej ako 3.3.5
Nuki Smart Lock 2.0 vo verzii staršej ako 2.12.4
Nuki Bridge v1 vo verzii staršej ako 1.22.0
Nuki Bridge v2 vo verzii staršej ako 2.13.2
Nuki Keypad vo verzii staršej ako 1.9.2
Nuki Fob vo verzii staršej ako 1.8.1
Nuki Smart Lock application vo verzii v2022.5.1 (661)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
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.securityweek.com/nuki-smart-lock-vulnerabilities-allow-hackers-open-doors https://research.nccgroup.com/2022/07/25/technical-advisory-multiple-vulnerabilities-in-nuki-smart-locks-cve-2022-32509-cve-2022-32504-cve-2022-32502-cve-2022-32507-cve-2022-32503-cve-2022-32510-cve-2022-32506-cve-2022-32508-cve-2/

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

Identifikátor

nVidia - viacero bezpečnostných zraniteľností

Popis

Spoločnosť nVidia vydala bezpečnostné aktualizácie na svoje portfólio grafických ovládačov, vGPU a Cloud Gaming softvéru, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia out-of-bounds prístupu k pamäti v kernel móde spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2022

CVE

CVE-2022-31606, CVE-2022-31607, CVE-2022-31608, CVE-2022-31609, CVE-2022-31610, CVE-2022-31612, CVE-2022-31613, CVE-2022-31614, CVE-2022-31615, CVE-2022-31616, CVE-2022-31617, CVE-2022-31618, CVE-2022-34665

Zasiahnuté systémy
Vetva ovládačov R515 pre GeForce na operačnom systéme Windows vo všetkých verziách
Vetva ovládačov R470 pre GeForce na operačnom systéme Windows 10 a 11 vo verzii staršej ako 473.81
Vetva ovládačov R470 pre GeForce na operačnom systéme Windows 7 a 8.x vo verzii staršej ako 473.81
Vetva ovládačov R515 pre Studio na operačnom systéme Windows vo všetkých verziách - dostupnosť aktualizácií plánovaná na 32. týždeň 2022
Vetva ovládačov R515 pre NVIDIA RTX/Quadro, NVS na operačnom systéme Windows vo verzii staršej ako 516.94
Vetva ovládačov R510 pre NVIDIA RTX/Quadro, NVS na operačnom systéme Windows vo verzii staršej ako 513.46
Vetva ovládačov R470 pre NVIDIA RTX/Quadro, NVS na operačnom systéme Windows vo verzii staršej ako 473.81
Vetva ovládačov R515 pre Tesla na operačnom systéme Windows vo verzii staršej ako 516.94
Vetva ovládačov R510 pre Tesla na operačnom systéme Windows vo verzii staršej ako 513.46
Vetva ovládačov R470 pre Tesla na operačnom systéme Windows vo verzii staršej ako 473.81
Vetva ovládačov R450 pre Tesla na operačnom systéme Windows vo verzii staršej ako 453.64
Vetva ovládačov R515 pre GeForce na operačnom systéme Linux vo verzii staršej ako 515.65.01
Vetva ovládačov R510 pre GeForce na operačnom systéme Linux vo verzii staršej ako 510.85.02
Vetva ovládačov R470 pre GeForce na operačnom systéme Linux vo verzii staršej ako 470.141.03
Vetva ovládačov R390 pre GeForce na operačnom systéme Linux vo verzii staršej ako 390.154
Vetva ovládačov R515 pre NVIDIA RTX, Quadro, NVS na operačnom systéme Linux vo verzii staršej ako 515.65.01
Vetva ovládačov R510 pre NVIDIA RTX, Quadro, NVS na operačnom systéme Linux vo verzii staršej ako 510.85.02
Vetva ovládačov R470 pre NVIDIA RTX, Quadro, NVS na operačnom systéme Linux vo verzii staršej ako 470.141.03
Vetva ovládačov R390 pre NVIDIA RTX, Quadro, NVS na operačnom systéme Linux vo verzii staršej ako 390.154
Vetva ovládačov R515 pre Tesla na operačnom systéme Linux vo verzii staršej ako 515.65.01
Vetva ovládačov R510 pre Tesla na operačnom systéme Linux vo verzii staršej ako 510.85.02
Vetva ovládačov R470 pre Tesla na operačnom systéme Linux vo verzii staršej ako 470.141.03
Vetva ovládačov R450 pre Tesla na operačnom systéme Linux vo verzii staršej ako 450.203.03
vGPU softvér pre Windows vo verzii staršej ako 14.2
vGPU softvér pre Windows vo verzii staršej ako 13.4
vGPU softvér pre Windows vo verzii staršej ako 11.9
vGPU softvér pre Linux vo verzii staršej ako 14.2
vGPU softvér pre Linux vo verzii staršej ako 13.4
vGPU softvér pre Citrix Hypervisor, VMware vSphere, Red Hat Enterprise Linux KVM vo verzii staršej ako 11.9
vGPU softvér pre Citrix Hypervisor, VMware vSphere, Red Hat Enterprise Linux KVM vo verzii staršej ako 14.2
vGPU softvér pre Citrix Hypervisor, VMware vSphere, Red Hat Enterprise Linux KVM vo verzii staršej ako 13.4
vGPU softvér pre Citrix Hypervisor, VMware vSphere, Red Hat Enterprise Linux KVM vo verzii staršej ako 11.9
NVIDIA Cloud Gaming pre Windows, Linux, Citrix Hypervisor, VMware vSphere, a Red Hat Enterprise Linux KVM vo všetkých verziách - dostupnosť aktualizácií plánovaná na 32. týždeň 2022

Následky
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje
https://nvidia.custhelp.com/app/answers/detail/a_id/5383/kw/security%20bulletin

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

Identifikátor

Kaspersky VPN Secure Connection - bezpečnostná zraniteľnosť

Popis

Spoločnosť Kaspersky vydala bezpečnostnú aktualizáciu na svoju virtuálnu privátnu sieť Kaspersky VPN Secure Connection, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia "Delete service data and reports" funkcie na zmazanie privilegovaného priečinka eskalovať svoje privilégiá a spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2022

CVE

CVE-2022-27535

Zasiahnuté systémy

Kaspersky VPN Secure Connection vo verzii staršej ako 21.7.7.393

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti 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.synopsys.com/blogs/software-security/cyrc-advisory-kasperksy-vpn-microsoft-windows/

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

Identifikátor

Apache Hadoop - bezpečnostná zraniteľnosť

Popis

Vývojári sofvérovej knižnice Apache Hadoop vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených argumentov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.08.2022

CVE

CVE-2022-25168

Zasiahnuté systémy

Apache Hadoop vo verzii staršej ako 2.10.2, 3.2.4, a 3.3.3

Následky

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

Odporúčania

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://exchange.xforce.ibmcloud.com/vulnerabilities/232807
https://hadoop.apache.org/cve_list.html

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

Identifikátor

Autodesk - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Autodesk vydala bezpečnostné aktualizácie na svoje portfólio produktov AutoCAD, Autodesk desktop app, Advance Steel, Civil 3D, Fusion, ReCap, Grading Optimization, InfraWorks Desktop, Arnold, Inventor, 3dsMAX, Revit a Navisworks, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom špeciálne vytvoreného odkazu eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2022

CVE

CVE-2021-22945, CVE-2021-22946, CVE-2021-22947, CVE-2021-45960, CVE-2021-46143, CVE-2022-0778, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315

Zasiahnuté systémy
Autodesk desktop app vo verzii staršej ako 8.5.0 Autodesk® AutoCAD® vo verzii staršej ako 2023.1 Autodesk® AutoCAD® LT vo verzii staršej ako 2023.1 Autodesk® AutoCAD® Architecture vo verzii staršej ako 2023.1** Autodesk® AutoCAD® Electrical vo verzii staršej ako 2023.1** Autodesk® AutoCAD® Map 3D vo verzii staršej ako 2023.1** Autodesk® AutoCAD® Mechanical vo verzii staršej ako 2023.1** Autodesk® AutoCAD® MEP vo verzii staršej ako 2023.1** Autodesk® AutoCAD® Plant 3D vo verzii staršej ako 2023.1** Autodesk® Advance Steel vo verzii staršej ako 2023.0.1** Autodesk® Civil 3D® vo verzii staršej ako 2023.1, 2022.1.3, 2021.3.1, 2020.6.2 Autodesk® Advance Steel vo verzii staršej ako 2023.1** Autodesk Fusion™ vo verzii staršej ako 2023.0.1** AutoCAD® Mac vo verzii staršej ako 7.1.2.0, 7.1.1.2 AutoCAD® LT for Mac vo verzii staršej ako 2023.0.1 ReCap® Pro vo verzii staršej ako 2023.0.1 Hotfix, 2022.2.1 Hotfix, 2021.1.3 Hotfix, 2020.2.3 Hotfix ReCap® Photo vo verzii staršej ako 2023.0.1 Hotfix, 2022.2.1 Hotfix, Grading Optimization vo verzii staršej ako 2021.2.1 Hotfix, 2020.3.1 Hotfix InfraWorks® Desktop vo verzii staršej ako 2023.0 Hotfix 1 Arnold® vo verzii staršej ako 2023.0.1, 2022.1.5 Inventor® vo verzii staršej ako 2023.0.1** 3dsMAX vo verzii staršej ako 2023.0.1** Revit® vo verzii staršej ako 2023.0.1** Navisworks® vo verzii staršej ako 2023.0.1**

Následky
Eskalácia privilégií 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.autodesk.com/trust/security-advisories/adsk-sa-2022-0016 https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0017 https://www.zerodayinitiative.com/advisories/ZDI-22-1035/

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

Identifikátor

F5 BIG-IP - viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj firewall BIG-IP, 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.

Dátum prvého zverejnenia varovania

03.08.2022

CVE

CVE-2022-30535, CVE-2022-31473, CVE-2022-32455, CVE-2022-33203, CVE-2022-33947, CVE-2022-33962, CVE-2022-33968, CVE-2022-34651, CVE-2022-34655, CVE-2022-34844, CVE-2022-34851, CVE-2022-34862, CVE-2022-34865, CVE-2022-35236, CVE-2022-35240, CVE-2022-35241, CVE-2022-35243, CVE-2022-35245, CVE-2022-35272, CVE-2022-35728, CVE-2022-35735

Zasiahnuté systémy

BIG-IP (všetky moduly) 17.x vo verzii staršej ako 17.0.0
BIG-IP (všetky moduly) 16.x vo verzii staršej ako 16.1.2.2
BIG-IP (všetky moduly) 15.x vo verzii staršej ako 15.1.6.1
BIG-IP (všetky moduly) 14.x vo verzii staršej ako 14.1.5
BIG-IP (všetky moduly) 13.x vo všetkých verziách

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/232726

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia funkcionality "TODO" získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

05.08.2022

CVE

CVE-2022-2095, CVE-2022-2303, CVE-2022-2307, CVE-2022-2326, CVE-2022-2417, CVE-2022-2456, CVE-2022-2459, CVE-2022-2497, CVE-2022-2498, CVE-2022-2499, CVE-2022-2500, CVE-2022-2501, CVE-2022-2512, CVE-2022-2531, CVE-2022-2534, CVE-2022-2539

Zasiahnuté systémy

GitLab Community Edition (CE) a Enterprise Edition (EE) vo verzii staršej ako 15.2.1, 15.1.4, a 15.0.5

Následky

Úplné narušenie dôvernosti 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://about.gitlab.com/releases/2022/07/28/security-release-gitlab-15-2-1-released/