BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 11. 2022 - 29. 11. 2022

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-951

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

Identifikátor

SolarWinds - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoju monitorovaciu platformu SolarWinds Platform, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.11.2022

CVE

CVE-2021-35246, CVE-2022-36960, CVE-2022-36962, CVE-2022-36964, CVE-2022-38113, CVE-2022-38114, CVE-2022-38115

Zasiahnuté systémy

SolarWinds Platform vo verzii staršej ako 2022.4

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.
Manažmentové rozhrania zariadení a serverov odporúčame nesprístupňovať z verejného Internetu.

Zdroje

https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36960
https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36964
https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36962
https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35246
https://www.solarwinds.com/trust-center/security-advisories/cve-2022-38115
https://www.solarwinds.com/trust-center/security-advisories/cve-2022-38114
https://www.solarwinds.com/trust-center/security-advisories/cve-2022-38113

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

Identifikátor

RubyGems cgi gem - viacero bezpečnostných zraniteľností

Popis

Vývojári knižnice cgi gem 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 zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.11.2022

CVE

CVE-2020-23587, CVE-2020-23588, CVE-2020-23592, CVE-2020-27216, CVE-2021-33621

Zasiahnuté systémy

cgi gem vo verzii staršej ako 0.1.0.2, 0.2.2, 0.3.5

Následky

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.redpacketsecurity.com/rubygems-cgi-gem-http-response-splitting-cve-2021-33621/

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

Identifikátor

MyBB - bezpečnostné zraniteľnosti

Popis

Vývojári softvéru na vytváranie fór MyBB vydali bezpečnostnú aktualizáciu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v SCEditore, spočíva v nedostatočej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného HTML kódu získať prístup k prihlasovacím údajom obete a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.11.2022

CVE

CVE-2022-43707, CVE-2022-43708, CVE-2022-43709

Zasiahnuté systémy

MyBB vo verzii staršej ako 1.8.32

Následky

Neoprávnený prístup k citlivým informáciám
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame 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 získanie prístupu k citlivým údajom alebo vykonanie škodlivého kódu 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://mybb.com/vo verzii od/1.8.32/
https://github.com/mybb/mybb/security/advisories/GHSA-6vpw-m83q-27px
https://exchange.xforce.ibmcloud.com/vulnerabilities/240558
https://exchange.xforce.ibmcloud.com/vulnerabilities/240557
https://exchange.xforce.ibmcloud.com/vulnerabilities/240554

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú tri bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch Factory Automation engineering software, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.11.2022

CVE

CVE-2020-14521, CVE-2021-20587, CVE-2021-20588

Zasiahnuté systémy
C Controller Interface Module utility vo verzii staršej ako 2.10
CC-Link IE Control Network Data Collector vo verzii staršej ako 1.01B
CC-Link IE Field Network Data Collector vo verzii staršej ako 1.01B
CC-Link IE TSN Data Collector vo verzii staršej ako 1.01B
CPU Module Logging Configuration Tool vo verzii staršej ako 1.118X
CW Configurator vo verzii staršej ako 1.012N
Data Transfer vo verzii staršej ako 3.45X
EZSocket vo verzii staršej ako 5.5
FR Configurator2 vo verzii staršej ako 1.25B
GT Designer3 Version1(GOT1000 vo verzii staršej ako 1.255R
GT Designer3 Version1(GOT2000 vo verzii staršej ako 1.255R
GT SoftGOT1000 Version3 vo verzii staršej ako 3.255R
GT SoftGOT2000 Version1 vo verzii staršej ako 1.255R
GX Developer vo verzii staršej ako 8.507D
GX LogViewer vo verzii staršej ako 1.118X
GX Works2 vo verzii staršej ako 1.600A
GX Works3 vo verzii staršej ako 1.072A
M_CommDTM-IO-Link vo verzii staršej ako 1.04E
MELFA-Works vo verzii staršej ako 4.5
MELSOFT Complete Clean Up Tool vo verzii staršej ako 1.07H
MELSOFT EM Software Development Kit (EM Configurator) vo verzii staršej ako 1.020W
MELSOFT iQ AppPortal vo verzii staršej ako 1.20W
MELSOFT Navigator vo verzii staršej ako 2.78G
MH11 SettingTool Version2 vo verzii staršej ako 2.005F
MI Configurator vo verzii staršej ako 1.005F
Motion Control Setting vo verzii staršej ako 1.006G
Motorizer vo verzii staršej ako 1.010L
MR Configurator2 vo verzii staršej ako 1.130L
MT Works2 vo verzii staršej ako 1.170C
MTConnect Data Collector vo verzii staršej ako 1.1.5.0
MX Component vo verzii staršej ako 5.002C
MX MESInterface vo verzii staršej ako 1.22Y
MX MESInterface-R vo verzii staršej ako 1.13P
MX Sheet vo verzii staršej ako 2.16S
Network Interface Board CC IE Control Utility vo verzii staršej ako 1.30G
Network Interface Board CC IE Field Utility vo verzii staršej ako 1.17T
Network Interface Board CC-Link Ver.2 Utility vo verzii staršej ako 1.24A
Network Interface Board MNETH Utility vo verzii staršej ako 35M
PX Developer vo verzii staršej ako 1.54G
RT ToolBox2 vo verzii staršej ako 3.74C
RT ToolBox3 vo verzii staršej ako 1.90U
Setting/monitoring tools for the C Controller module (SW3PVC-CCPU) vo verzii staršej ako 3.14Q
Setting/monitoring tools for the C Controller module (SW4PVC-CCPU) vo verzii staršej ako 4.13P
SLMP Data Collector vo verzii staršej ako 1.05F

Následky
Zneprístupnenie služby
Neoprávnený prístup k citlivým informáciám
Neoprávnené zmeny v systéme

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu. Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-007_en.pdf
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2020-021_en.pdf
https://www.cisa.gov/uscert/ics/advisories/icsa-21-049-02
https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-04

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

Identifikátor

Foxit PDF Reader - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoj produkt Foxit PDF Reader, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.11.2022

CVE

CVE-2022-43637, CVE-2022-43638, CVE-2022-43639, CVE-2022-43640, CVE-2022-43641

Zasiahnuté systémy

Foxit PDF Editor for Mac 11.1.4
Foxit PDF Reader 12.0.2
Foxit PDF Editor 12.0.2

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://www.zerodayinitiative.com/advisories/ZDI-22-1657/
https://www.foxit.com/support/security-bulletins.html

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

Identifikátor

Phoenix Contact Automation Worx Software Suite - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Phoenix Contact vydala bezpečnostnú aktualizáciu na svoj softvérový balík Automation Worx Software Suite, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.11.2022

CVE

CVE-2022-3461, CVE-2022-3737

Zasiahnuté systémy

Automation Worx Software Suite vo verzii staršej ako 1.89

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.cisa.gov/uscert/ics/advisories/icsa-22-326-03
https://cert.vde.com/en/advisories/VDE-2022-048/

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

Identifikátor

Moxa ARM zariadenia - bezpečnostná zraniteľnosť

Popis

Spoločnosť Moxa vydala bezpečnostné aktualizácie na svoje zariadenia s ARM procesorom, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

22.11.2022

CVE

CVE-2022-3088

Zasiahnuté systémy

UC-8100A-ME-T System Image vo verzii od v1.0 do v1.6 (vrátane)
UC-2100 System Image vo verzii od v1.0 do v1.12 (vrátane)
UC-2100-W System Image vo verzii od v1.0 do v 1.12 (vrátane)
UC-3100 System Image vo verzii od v1.0 do v1.6 (vrátane)
UC-5100 System Image vo verzii od v1.0 do v1.4 (vrátane)
UC-8100 System Image vo verzii od v3.0 do v3.5 (vrátane)
UC-8100-ME-T System Image vo verziách v3.0 a v3.1
UC-8100A-ME-T System Image vo verzii od v1.0 do v1.6 (vrátane)
UC-8200 System Image vo verzii od v1.0 do v1.5 (vrátane)
AIG-300 System Image vo verzii od v1.0 do v1.4 (vrátane)
UC-8410A with Debian 9 System Image: vo verziách v4.0.2 a v4.1.2
UC-8580 with Debian 9 System Image: vo verzii od v2.0 a v2.1
UC-8540 with Debian 9 System Image: vo verzii od v2.0 a v2.1
DA-662C-16-LX (GLB) System Image: vo verzii od v1.0.2 do v1.1.2

Následky

Eskalácia privilégií
Získanie úplnej kontroly nad systémom

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pre produkty zo sérií UC a DA aplikujte bezpečnostné aktualizácie postupom podľa návodu na stránke výrobcu (presný odkaz v sekcii ZDROJE) v sekcii "UC and DA Series" a pre produkty zo série AIG-300 inštalujte nástroj ThingsPro Proxy postupom podľa návodu na spomínanej stránke výrobcu v sekcii "AIG-300 Series". Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od internetu. 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/moxa-arm-based-computer-improper-privilege-management-vulnerability https://www.cisa.gov/uscert/ics/advisories/icsa-22-326-05

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

Identifikátor

PILZ PASvisu - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť PILZ vydala bezpečnostnú aktualizáciu na svoj human-machine interface softvér PASvisu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

24.11.2022

CVE

CVE-2022-25299, CVE-2022-40977

Zasiahnuté systémy

PASvisu Software < 1.12.0
PMI v5xx vo verzii staršej ako (vrátane) 1.3.58
PMI v7xx vo verzii staršej ako 2.2.0
PMI v8xx vo verzii staršej ako 1.6.102

Následky

Neoprávnená zmena v systéme

Odporúčania

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

Zdroje

https://cert.vde.com/en/advisories/VDE-2022-033/

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

Identifikátor

HPE Aruba EdgeConnect Enterprise - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na svoj produkt Aruba EdgeConnect Enterprise ECOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v API webového rozhrania, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.11.2022

CVE

CVE-2022-37919, CVE-2022-37920, CVE-2022-37921, CVE-2022-37922, CVE-2022-37923, CVE-2022-37924, CVE-2022-37925, CVE-2022-37926, CVE-2022-43518, CVE-2022-43541, CVE-2022-43542, CVE-2022-44532, CVE-2022-44533

Zasiahnuté systémy

HPE Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.2.2.0
HPE Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.1.4.0
HPE Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 9.0.8.0
HPE Aruba EdgeConnect Enterprise ECOS vo verzii staršej ako 8.3.8.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04389en_us

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TensorFlow - viacero bezpečnostných zraniteľností

Popis

Vývojári knižnice TensorFlow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom out-of-bound zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.11.2022

CVE

CVE-2022-41880, CVE-2022-41883, CVE-2022-41884, CVE-2022-41885, CVE-2022-41886, CVE-2022-41887, CVE-2022-41888, CVE-2022-41889, CVE-2022-41890, CVE-2022-41891, CVE-2022-41893, CVE-2022-41894, CVE-2022-41895, CVE-2022-41896, CVE-2022-41897, CVE-2022-41898, CVE-2022-41899, CVE-2022-41900, CVE-2022-41901, CVE-2022-41907

Zasiahnuté systémy

TensorFlow vo verzii staršej ako 2.8.4, 2.9.3, 2.10.1, 2.11.0

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú predmetnú knižnicu 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://security.snyk.io/vuln/SNYK-PYTHON-TENSORFLOWGPU-3136507
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xf83-q765-xm6m
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cqvq-fvhr-v6hc
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-frqp-wp83-qggv
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pf36-r9c6-h97j
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rjx6-v474-2ch9
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv77-9g28-cwg3
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-368v-7v32-52fx
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cg88-rpvp-cjv5
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9fm-r5mm-rf9f
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xvwp-h6jv-7472
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-27rc-728f-x5w2
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-hq7g-wwwp-q46h
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f2w8-jw48-fr7j
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rmg2-f698-wq35
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gq2j-cr96-gvqx
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h6q3-vv32-2cq5
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-67pf-62xr-q35m
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-66vq-54fq-6jvv
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h246-cgh4-7475
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-xxcj-rhqg-m46g
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6x99-gv2v-q76v
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8fvv-46hw-vpg3
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-54pp-c6pp-7fpx
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-762h-vpvw-3rcx
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jq6x-99hj-q636
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w58w-79xv-6vcj
https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8w5g-3wcv-9g2j