BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 02. 2021 - 02. 03. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Viacero bezpečnostných zraniteľností v produktoch Mozilla	Vysoká	**8.8**
02.	Bezpečnostné zraniteľnosti v produkte Directus	Vysoká	**8.8**
03.	Bezpečnostná zraniteľnosť v produktoch Netgear	Vysoká	**8.8**
04.	Bezpečnostné zraniteľnosti v produkte TP-Link Archer A7 AC1750	Vysoká	**8.8**
05.	Bezpečnostná zraniteľnosť v produkte PerFact OpenVPN-Client	Vysoká	**8.8**
06.	Bezpečnostná zraniteľnosť v produktoch ProSoft Technology ICX35-HWC	Vysoká	**8.2**
07.	Bezpečnostná zraniteľnosť v produkte Red Hat OpenShift Installer	Vysoká	**8.1**
08.	Bezpečnostná zraniteľnosť v produkte Dell EMC PowerProtect Cyber Recovery	Vysoká	**7.9**
09.	Bezpečnostné zraniteľnosti v produktoch Bosch	Vysoká	**7.8**
10.	Bezpečnostná zraniteľnosť v produkte SolarWinds Patch Manager	Vysoká	**7.8**
11.	Viacero bezpečnostných zraniteľností v produkte Fatek FvDesigner	Vysoká	**7.8**
12.	Bezpečnostná zraniteľnosť v produkte Isync	Vysoká	**7.5**
13.	Bezpečnostná zraniteľnosť v produkte Stunnel	Vysoká	**7.5**
14.	Bezpečnostná zraniteľnosť v produkte OpenRepeater	Vysoká	**7.3**

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:
01439/2020/SK-CERT-355

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Mozilla

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 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

23.02.2021

CVE

CVE-2020-26954, CVE-2021-23968, CVE-2021-23969, CVE-2021-23970, CVE-2021-23971, CVE-2021-23972, CVE-2021-23973, CVE-2021-23974, CVE-2021-23975, CVE-2021-23976, CVE-2021-23977, CVE-2021-23978, CVE-2021-23979

Zasiahnuté systémy

Mozilla Thunderbird vo verzii staršej ako 78.8
Mozilla Firefox ESR vo verzii staršej ako 78.8
Mozilla Firefox vo verzii staršej ako 86

Následky

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

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 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.mozilla.org/en-US/security/advisories/mfsa2021-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-07/
https://exchange.xforce.ibmcloud.com/vulnerabilities/197286

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

Identifikátor

Bezpečnostné zraniteľnosti v produkte Directus

Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých zraniteľnostiach produktu Directus.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.02.2021

CVE

CVE-2021-26593, CVE-2021-26594, CVE-2021-26595

Zasiahnuté systémy

Directus Directus vo verzii staršej ako 8.8.1 (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/197311
https://exchange.xforce.ibmcloud.com/vulnerabilities/197309
https://exchange.xforce.ibmcloud.com/vulnerabilities/197312
https://github.com/sgranel/directusv8

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Netgear

Popis

Spoločnosť Netgear vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente, prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.02.2021

CVE

CVE-2021-27239

Zasiahnuté systémy

D6220 s firmware vo verzii staršej ako 1.0.0.68
D6400 s firmware vo verzii staršej ako 1.0.0.102
D7000v2 s firmware vo verzii staršej ako 1.0.0.66
D8500 s firmware vo verzii staršej ako1.0.3.60
DC112A s firmware vo verzii staršej ako 1.0.0.54
EX7000 s firmware vo verzii staršej ako 1.0.1.94
EX7500 s firmware vo verzii staršej ako 1.0.0.72
R6250 s firmware vo verzii staršej ako 1.0.4.48
R6300v2 s firmware vo verzii staršej ako 1.0.4.50
R6400 s firmware vo verzii staršej ako 1.0.1.68
R6400v2 s firmware vo verzii staršej ako 1.0.4.102
R6700v3 s firmware vo verzii staršej ako 1.0.4.102
R6900P s firmware vo verzii staršej ako 1.3.2.132
R7000 s firmware vo verzii staršej ako 1.0.11.116
R7000P s firmware vo verzii staršej ako 1.3.2.132
R7100LG s firmware vo verzii staršej ako 1.0.0.64
R7850 s firmware vo verzii staršej ako 1.0.5.68
R7900 sfirmware vo verzii staršej ako 1.0.4.38
R7900P s firmware vo verzii staršej ako 1.4.1.68
R7960P s firmware vo verzii staršej ako 1.4.1.68
R8000 s firmware vo verzii staršej ako 1.0.4.68
R8000P s firmware vo verzii staršej ako 1.4.1.68
R8300 s firmware vo verzii staršej ako 1.0.2.144
R8500 s firmware vo verzii staršej ako 1.0.2.144
RAX200 s firmware vo verzii staršej ako 1.0.2.88
RAX75 s firmware vo verzii staršej ako 1.0.3.102
RAX80 s firmware vo verzii staršej ako 1.0.3.102
RBR750 s firmware vo verzii staršej ako 3.2.17.12
RBR850 s firmware vo verzii staršej ako 3.2.17.12
RBS40V s firmware vo verzii staršej ako 2.6.2.4
RBS750 s firmware vo verzii staršej ako 3.2.17.12
RBS850 s firmware vo verzii staršej ako 3.2.17.12
RS400 s firmware vo verzii staršej ako 1.5.0.68_hotfix
WNDR3400v3 s firmware vo verzii staršej ako 1.0.1.38
WNR3500Lv2 s firmware vo verzii staršej ako 1.2.0.66
XR300 s firmware vo verzii staršej ako 1.0.3.56

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://exchange.xforce.ibmcloud.com/vulnerabilities/197375
https://kb.netgear.com/000062820/Security-Advisory-for-Stack-based-Buffer-Overflow-Remote-Code-Execution-Vulnerability-on-Some-Routers-PSV-2020-0432
https://www.zerodayinitiative.com/advisories/ZDI-21-206/

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

Identifikátor

Bezpečnostné zraniteľnosti v produkte TP-Link Archer A7 AC1750

Popis

Spoločnosť TP-Link vydala bezpečnostné aktualizácie na produkt Archer A7 AC1750, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne vytvoreného TCP paketu, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.02.2021

CVE

CVE-2021-27245, CVE-2021-27246

Zasiahnuté systémy

Archer A7 AC1750 vo verzii staršej ako V5_210125

Následky

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

Odporúčania

Administrátorom 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://exchange.xforce.ibmcloud.com/vulnerabilities/197381
https://exchange.xforce.ibmcloud.com/vulnerabilities/197380
https://www.tp-link.com/us/home-networking/wifi-router/archer-a7/

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte PerFact OpenVPN-Client

Popis

Spoločnosť PerFact vydala bezpečnostnú aktualizáciu na svoj produkt OpenVPN-Client, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených konfiguračných príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.02.2021

CVE

CVE-2021-27406

Zasiahnuté systémy

OpenVPN-Client vo verzii staršej ako 1.6.0

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://us-cert.cisa.gov/ics/advisories/icsa-21-056-01

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch ProSoft Technology ICX35-HWC

Popis

Spoločnosť ProSoft Technology vydala bezpečnostné aktualizácie na produkty ICX35-HWC-A a ICX35-HWC-E, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.02.2021

CVE

CVE-2021-22661

Zasiahnuté systémy

ICX35-HWC-A vo verzii staršej ako 1.10.30
ICX35-HWC-E vo verzii staršej ako 1.10.30

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-056-04
https://www.prosoft-technology.com/Products/Industrial-Wireless/Intelligent-Cellular/Industrial-Cellular-Gateway-ICX35-HWC

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Red Hat OpenShift Installer

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj produkt OpenShift Installer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.02.2021

CVE

CVE-2021-20198

Zasiahnuté systémy

OpenShift Installer vo verzii staršej ako 0.9.0-master.0.20210125200451-95101da940b0

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://exchange.xforce.ibmcloud.com/vulnerabilities/197308
https://bugzilla.redhat.com/show_bug.cgi?id=1920764
https://github.com/openshift/installer/pull/4590

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Dell EMC PowerProtect Cyber Recovery

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt EMC PowerProtect Cyber Recovery, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.02.2021

CVE

CVE-2021-21512

Zasiahnuté systémy

Dell EMC PowerProtect Cyber Recovery vo verzii staršej ako 19.7.0.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://exchange.xforce.ibmcloud.com/vulnerabilities/197123
https://www.dell.com/support/kbdoc/sk-sk/000183169/dsa-2021-038-dell-emc-powerprotect-cyber-recovery-security-update-for-unintended-information-disclosure
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21512
https://www.delltechnologies.com/en-us/collaterals/unauth/offering-overview-documents/products/data-protection/isolated-recovery-solution-overview.pdf

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

Identifikátor

Bezpečnostné zraniteľnosti v produktoch Bosch

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov Rexroth IoT Gateway a ctrlX CORE Runtime.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.02.2021

CVE

CVE-2020-29661, CVE-2021-3156, CVE-2021-3347

Zasiahnuté systémy

Rexroth IoT Gateway s IndraControl PR21: PR2100.1-*-IOTNN všetky verzie
ctrlX CORE Runtime < XCR-V-0108 všetky verzie

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-372917.html

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte SolarWinds Patch Manager

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt Patch Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.02.2021

CVE

CVE-2021-27240

Zasiahnuté systémy

SolarWinds Patch Manager vo verzii staršej ako 2020.2.4

Následky

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

Odporúčania

Administrátorom 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://exchange.xforce.ibmcloud.com/vulnerabilities/197376
https://www.solarwinds.com/patch-manager
https://www.zerodayinitiative.com/advisories/ZDI-21-207/

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

Identifikátor

Viacero bezpečnostných zraniteľností v produkte Fatek FvDesigner

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu FvDesigner.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.02.2021

CVE

CVE-2021-22638, CVE-2021-22662, CVE-2021-22666, CVE-2021-22670, CVE-2021-22683

Zasiahnuté systémy

FvDesigner Version vo verzii staršej ako 1.5.76 (vrátane)

Následky

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 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://us-cert.cisa.gov/ics/advisories/icsa-21-056-02

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Isync

Popis

Vývojári balíka Isync vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej validácii názvu emailovej schránky vrátenej mbsync príkazom IMAP LIST/LSUB a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej emailovej schránky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.02.2021

CVE

CVE-2021-20247

Zasiahnuté systémy

Isync vo verzii staršej ako 1.3.5
Isync vo verzii staršej ako 1.4.1

Následky

Neoprávnený prístup k citlivým údajom

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://exchange.xforce.ibmcloud.com/vulnerabilities/197131
https://seclists.org/oss-sec/2021/q1/170
https://sourceforge.net/projects/isync/

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Stunnel

Popis

Vývojári programu Stunnel 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 vytvoreného certifikátu získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.02.2021

CVE

CVE-2021-20230

Zasiahnuté systémy

Stunnel vo verzii staršej ako 5.57

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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://exchange.xforce.ibmcloud.com/vulnerabilities/197302
https://bugzilla.redhat.com/show_bug.cgi?id=1925226
https://github.com/mtrojnar/stunnel/commit/ebad9ddc4efb2635f37174c9d800d06206f1edf9

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte OpenRepeater

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu OpenRepeater.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.02.2021

CVE

CVE-2019-25024

Zasiahnuté systémy

OpenRepeater vo verzii staršej ako 2.1 (vrátane)

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/197108
https://github.com/codexlynx/CVE-2019-25024
https://github.com/OpenRepeater/openrepeater/issues/66
https://www.tenable.com/cve/CVE-2019-25024
https://github.com/OpenRepeater

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:
01439/2020/SK-CERT-355