BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 01. 2021 - 02. 02. 2021

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:
01439/2020/SK-CERT-322

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Klog Server

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Klog Server.
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

26.01.2021

CVE

CVE-2021-3317

Zasiahnuté systémy

Klog Server vo verzii staršej ako 2.4.1 (vrátane)

Následky

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

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/195743
https://docs.unsafe-inline.com/0day/klog-server-authenticated-command-injection
https://www.klogserver.com/

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Fuji Electric Tellus Lite V-Simulator a V-Server Lite

Popis

Spoločnosť Fuji Electric vydala bezpečnostné aktualizácie na svoje produkty Tellus Lite V-Simulator a V-Server Lite, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.01.2021

CVE

CVE-2021-22637, CVE-2021-22639, CVE-2021-22641, CVE-2021-22653, CVE-2021-22655

Zasiahnuté systémy

Tellus Lite V-Simulator vo verzii staršej ako 4.0.10.0
V-Server Lite vo verzii staršej ako 4.0.10.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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-21-026-01

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Mozilla Firefox a Thunderbird

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému,
neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.01.2021

CVE

CVE-2020-15685, CVE-2020-26976, CVE-2021-23953, CVE-2021-23954, CVE-2021-23955, CVE-2021-23956, CVE-2021-23957, CVE-2021-23958, CVE-2021-23959, CVE-2021-23960, CVE-2021-23961, CVE-2021-23962, CVE-2021-23963, CVE-2021-23964, CVE-2021-23965

Zasiahnuté systémy

Mozilla Firefox vo verzii staršej ako 85
Mozilla Firefox ESR vo verzii staršej ako 78.7
Mozilla Thunderbird vo verzii staršej ako 78.7

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.mozilla.org/en-US/security/advisories/mfsa2021-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/
https://access.redhat.com/security/cve/CVE-2021-23953
https://www.tenable.com/plugins/nessus/145466
https://access.redhat.com/errata/RHSA-2021:0288

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Rockwell FactoryTalk

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov FactoryTalk Linx a FactoryTalk Services Platform.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.01.2021

CVE

CVE-2020-5801, CVE-2020-5802, CVE-2020-5806, CVE-2020-5807

Zasiahnuté systémy

FactoryTalk Linx software vo verzii staršej ako 6.20 (vrátane)
FactoryTalkServices Platform vo verzii staršej ako 6.20 (vrátane)

Následky

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-028-01

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch DH2i DxEnterprise a DxOdyssey

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov DH2i DxEnterprise a DxOdyssey.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

29.01.2021

CVE

CVE-2021-3341

Zasiahnuté systémy

DH2i DxEnterprise pre Windows vo verzii staršej ako 20.0.218 (vrátane)
DH2i DxOdyssey pre Windows vo verzii staršej ako 20.0.219 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedeú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Administrátorom taktiež odporúčame do vydania bezpečnostných záplat zastaviť a následne zakázať komponent DxWebEngine, ktorý nemá vplyv na funkcionalitu DxEnterprise a DxOdyssey.
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/195805
https://clients.dh2i.com/Support/Article.aspx?ID=2963454
https://dh2i.com/dxenterprise/

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Mitsubishi Electric

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje portfóilio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

26.01.2021

CVE

CVE-2020-16226

Zasiahnuté systémy

QJ71MES96 všetky verzie, QJ71WS96 všetky verzie
Q06CCPU-V všetky verzie, Q24DHCCPU-V všetky verzie
Q24DHCCPU-VG všetky verzie, R12CCPU-V vo verzii staršej ako 14
RD55UP06-V vo verzii staršej ako 10, RD55UP12-V vo verzii staršej ako 02
RJ71GN11-T2 vo verzii staršej ako 12, RJ71EN71 všetky verzie
QJ71E71-100 všetky verzie, LJ71E71-100 všetky verzie
QJ71MT91 všetky verzie, RD78G4 všetky verzie, RD78G8 všetky verzie, RD78G16 všetky verzie
RD78G32 všetky verzie, RD78G64 všetky verzie, RD78GHV všetky verzie, RD78GHW všetky verzie
NZ2GACP620-60 všetky verzie, NZ2GACP620-300 všetky verzie
NZ2FT-MT všetky verzie, NZ2FT-EIP všetky verzie
Q03UDECPU vo verzii staršej ako 22082
Q04UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q06UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q10UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q13UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q20UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q26UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q50UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q100UDEHCPU vo verzii staršej ako 22082 (prvých 5 číslic sériového čísla)
Q03UDVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q04UDVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q06UDVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q13UDVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q26UDVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q04UDPVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q06UDPVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q13UDPVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
Q26UDPVCPU vo verzii staršej ako 22032 (prvých 5 číslic sériového čísla)
L02CPU(-P) vo verzii staršej ako 22052 (prvých 5 číslic sériového čísla)
L06CPU(-P) vo verzii staršej ako 22052 (prvých 5 číslic sériového čísla)
L26CPU(-P) vo verzii staršej ako 22052 (prvých 5 číslic sériového čísla)
L26CPU-(P)BT vo verzii staršej ako 22052 (prvých 5 číslic sériového čísla)
R00CPU vo verzii staršej ako 19, R01CPU vo verzii staršej ako 19
R02CPU vo verzii staršej ako 19, RnCPU vo verzii staršej ako 51
RnENCPU vo verzii staršej ako 51, RnSFCPU vo verzii staršej ako 23
RnPCPU vo verzii staršej ako 25, RnPSFCPU vo verzii staršej ako 06
FX5U(C)- so sériovým číslom 17X**** vo verzii staršej ako 1.211
FX5U(C)- so sériovým číslom 179**** vo verzii staršej ako 1.071
FX5UC- so sériovým číslom 32M*/**-TS vo verzii staršej ako 1.211
FX5UJ- so sériovým číslom **M*/** vo verzii staršej ako 1.001
FX5-ENET vo verzii staršej ako 1.003
FX5-ENET/IP vo verzii staršej ako 1.23
FX3U-ENET-ADP vo verzii staršej ako 1.24
FX3GE všetky verzie
FX3U-ENET vo verzii staršej ako 1.16
FX3U-ENET-L vo verzii staršej ako 1.16
FX3U-ENET-P502 vo verzii staršej ako 1.16
FX5-CCLGN-MS vo verzii staršej ako 1.001
IU1-1M20-D všetky verzie, LE7-40GU-L všetky verzie
GOT2000 Series GT21 Model všetky verzie
GOT1000 Series GT14 Model všetky verzie
GT25-J71GN13-T2 všetky verzie, GS Series všetky verzie
FR-A800-E vo verzii staršej ako 01.01.2021, FR-F800-E vo verzii staršej ako 01.01.2021
FR-A8NCG vo verzii staršej ako 01.09.2020, FR-E800-EPA vo verzii staršej ako 01.09.2020
FR-E800-EPB vo verzii staršej ako 01.09.2020
Conveyor Tracking Application APR-nTR3FH všetky verzie (ukončená podpora)
Conveyor Tracking Application APR-nTR6FH všetky verzie (ukončená podpora)
Conveyor Tracking Application APR-nTR12FH všetky verzie (ukončená podpora)
Conveyor Tracking Application APR-nTR20FH všetky verzie (ukončená podpora)
MR-JE-C všetky verzie, MR-J4-TM všetky verzie

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-322

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

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. 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-20-245-01