BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 04. 2021 - 13. 04. 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-387

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

Identifikátor

Google Android OS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu operačného systému Android OS, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii 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

05.04.2021

CVE

CVE-2020-11191, CVE-2020-11210, CVE-2020-11234, CVE-2020-11236, CVE-2020-11237, CVE-2020-11242, CVE-2020-11243, CVE-2020-11245, CVE-2020-11246, CVE-2020-11247, CVE-2020-11251, CVE-2020-11252, CVE-2020-11255, CVE-2020-15436, CVE-2020-25705, CVE-2021-0400, CVE-2021-0426, CVE-2021-0427, CVE-2021-0428, CVE-2021-0429, CVE-2021-0430, CVE-2021-0431, CVE-2021-0432, CVE-2021-0433, CVE-2021-0435, CVE-2021-0436, CVE-2021-0437, CVE-2021-0438, CVE-2021-0439, CVE-2021-0442, CVE-2021-0443, CVE-2021-0444, CVE-2021-0445, CVE-2021-0446, CVE-2021-0468, CVE-2021-0471

Zasiahnuté systémy

Google Android OS vo verzii staršej ako Security patch 2021-04-05

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://source.android.com/security/bulletin/2021-04-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-remote-code-execution_2021-043/
https://www.cybersecurity-help.cz/vdb/SB2021040502
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

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

Identifikátor

Mark Text - bezpečnostná zraniteľnosť

Popis

Vývojári markdown editoru Mark Text vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

04.04.2021

CVE

CVE-2021-29996

Zasiahnuté systémy

Mark Text vo verzii staršej ako 0.16.3 (vrátane)

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://exchange.xforce.ibmcloud.com/vulnerabilities/199392
https://marktext.app/
https://github.com/marktext/marktext/issues/2548

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

Identifikátor

Jenkins produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Jenkins vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.04.2021

CVE

CVE-2021-21639, CVE-2021-21640, CVE-2021-21641, CVE-2021-22510, CVE-2021-22511, CVE-2021-22512, CVE-2021-22513

Zasiahnuté systémy

Jenkins weekly vo verzii staršej ako 2.287
Jenkins LTS vo verzii staršej ako 2.277.2
Micro Focus Application Automation Tools Plugin vo verzii staršej ako 6.8
Promoted builds Plugin vo verzii staršej ako 3.9.1

Následky

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

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://exchange.xforce.ibmcloud.com/vulnerabilities/199543
https://www.jenkins.io/security/advisory/2021-04-07/

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

Identifikátor

FATEK Automation WinProladder produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť FATEK Automation vydala bezpečnostnú aktualizáciu na svoj produkt WinProladder, ktorá opravuje bezpečnostnú zraniteľnosť.
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

08.04.2021

CVE

CVE-2021-2748

Zasiahnuté systémy

FATEK Automation WinProladder vo verzii staršej ako 3.30 (vrátane)

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.
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-21-098-01

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

Identifikátor

Apache CXF produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt CXF, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby autorizačného servera.

Dátum prvého zverejnenia varovania

02.04.2021

CVE

CVE-2021-22696

Zasiahnuté systémy

Apache CXF vo verzii staršej ako 3.3.10
Apache CXF vo verzii staršej ako 3.4.3

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú Apache CXF v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/199335
https://seclists.org/oss-sec/2021/q2/2
https://cxf.apache.org/

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

Identifikátor

Eclipse Jetty produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Eclipse vydala bezpečnostnú aktualizáciu na svoj produkt Jetty, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených TLS rámcov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.04.2021

CVE

CVE-2021-28165

Zasiahnuté systémy

Eclipse Jetty vo verzii staršej ako 9.4.39
Eclipse Jetty vo verzii staršej ako 10.0.2
Eclipse Jetty vo verzii staršej ako 11.0.2

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na Eclipse Jetty v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/199305
https://github.com/eclipse/jetty.project/security/advisories/GHSA-26vr-8j45-3r4w

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

Identifikátor

Hitachi ABB Power Grids - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.04.2021

CVE

CVE-2021-27196

Zasiahnuté systémy

PWC600 vo verzii 1.0.1.4
PWC600 vo verzii 1.1.0.1
GMS600 vo verzii 1.3.1
MSM vo verzii staršej ako 2.1.0+
FOX615 TEGO1 vo verzii staršej ako R2A16 (vrátane)
REB500 vo verzii 7.60.19
REB500 vo verzii 8.2.0.5
REB500 vo verzii 8.3.1.0
REB500 vo verzii staršej ako 7.60.19
RTU500 CMU firmware vo verzii staršej ako 12.6.1.0
RTU500 CMU firmware vo verzii staršej ako 12.4.10.0
RTU500 CMU firmware vo verzii staršej ako 12.2.11.0
RTU500 CMU firmware vo verzii staršej ako 12.0.14.0
RTU500 vo verzii staršej ako 12
Relion 670 vo verzii staršej ako 1.1
Relion 670 vo verzii staršej ako 1.2.3.20
Relion 670 vo verzii staršej ako 2.0
Relion 670 vo verzii staršej ako 2.1
Relion 670/650 vo verzii staršej ako 2.2.0.13
Relion 670/650/SAM600-IO vo verzii staršej ako 2.2.1.6
Relion 670 vo verzii staršej ako 2.2.2.3
Relion 670 vo verzii staršej ako 2.2.3.2
Relion 650 vo verzii staršej ako 1.2
Relion 650 vo verzii staršej ako 1.3.0.7

Následky

Zneprístupnenie služby

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

Zdroje
https://us-cert.cisa.gov/ics/advisories/icsa-21-096-01

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

Identifikátor

Dnsmasq produkt - bezpečnostná zraniteľnosť

Popis

Vývojári programu dnsmasq vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať DNS Cache Poisoning útok.

Dátum prvého zverejnenia varovania

08.04.2021

CVE

CVE-2021-3448

Zasiahnuté systémy

dnsmasq vo verzii staršej ako 2.85

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://bugzilla.redhat.com/show_bug.cgi?id=1939368
https://thekelleys.org.uk/gitweb/?p=dnsmasq.git;a=commit;h=74d4fcd756a85bc1823232ea74334f7ccfb9d5d2

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Froala WYSIWYG Editor - bezpečnostná zraniteľnosť

Popis

Vývojári WYSIWYG editoru Froala vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať XSS útok a následne získať neoprávnený prístup k citlivým údajom uloženým v cookies.

Dátum prvého zverejnenia varovania

05.04.2021

CVE

CVE-2021-30109

Zasiahnuté systémy

Froala WYSIWYG Editor vo verzii staršej ako V3.2.6 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú Froala WYSIWYG editor v zraniteľných verziách. V prípade, že áno, do vydania bezpečnostných aktualizácií odporúčame editor nepoužívať. Po vydaní bezpečnostných záplat 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/199384
https://github.com/Hackdwerg/CVE-2021-30109/blob/main/README.md
https://froala.com/wysiwyg-editor/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Seafile produkt - bezpečnostná zraniteľnosť

Popis

Vývojári programu Seafile vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať XSS útok a získať neoprávnený prístup k citlivým údajom uloženým v cookies.

Dátum prvého zverejnenia varovania

06.04.2021

CVE

CVE-2021-30146

Zasiahnuté systémy

Seafile vo verzii staršej ako 8.0.1 beta

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/199509
https://github.com/Security-AVS/CVE-2021-30146

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ASUS produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť ASUS vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.04.2021

CVE

CVE-2021-28183, CVE-2021-28184, CVE-2021-28185, CVE-2021-28186, CVE-2021-28187, CVE-2021-28188, CVE-2021-28189, CVE-2021-28190, CVE-2021-28191, CVE-2021-28192, CVE-2021-28203, CVE-2021-28204, CVE-2021-28205, CVE-2021-28206, CVE-2021-28207, CVE-2021-28208, CVE-2021-28209

Zasiahnuté systémy
Z10PR-D16 vo verzii staršej ako 1.16.1
ASMB8-iKVM vo verzii staršej ako 1.16.1
Z10PE-D16 WS vo verzii staršej ako 1.16.1
ASMB9-iKVM vo verzii staršej ako 1.15.3
RS700-E9-RS4 vo verzii staršej ako 1.15.4
ESC4000 G4X vo verzii staršej ako 1.15.6
RS700-E9-RS12 vo verzii staršej ako 1.15.4
RS100-E10-PI2 vo verzii staršej ako 1.15.3
RS300-E10-PS4 vo verzii staršej ako 1.15.3
RS300-E10-RS4 vo verzii staršej ako 1.15.3
RS500A-E9-PS4 vo verzii staršej ako 1.14.2
RS500A-E9-RS4 vo verzii staršej ako 1.14.2
RS500A-E9 RS4 U vo verzii staršej ako 1.14.2
E700 G4 vo verzii staršej ako 1.14.2
WS C422 PRO/SE vo verzii staršej ako 1.14.2
WS X299 PRO/SE vo verzii staršej ako 1.14.2
Z11PA-U12 vo verzii staršej ako 1.15.2
Z11PA-U12/10G-2S vo verzii staršej ako 1.15.2
KNPA-U16 vo verzii staršej ako 1.14.5
ESC4000 DHD G4 vo verzii staršej ako 1.15.2
ESC4000 G4 vo verzii staršej ako 1.15.6
RS720Q-E9-RS24-S vo verzii staršej ako 1.15.1
RS720Q-E9-RS8 vo verzii staršej ako 1.15.1
RS720Q-E9-RS8-S vo verzii staršej ako 1.15.1
Z11PA-D8 vo verzii staršej ako 1.15.2
Z11PA-D8C vo verzii staršej ako 1.15.2
RS720-E9-RS24-U vo verzii staršej ako 1.15.5
RS720-E9-RS8-G vo verzii staršej ako 1.15.4
RS500-E9-PS4 vo verzii staršej ako 1.15.5
Pro E800 G4 vo verzii staršej ako 1.15.2
RS500-E9-RS4 vo verzii staršej ako 1.15.5
RS500-E9-RS4-U vo verzii staršej ako 1.15.5
RS520-E9-RS12-E vo verzii staršej ako 1.15.4
RS520-E9-RS8 vo verzii staršej ako 1.15.4
ESC8000 G4 vo verzii staršej ako 1.15.5
ESC8000 G4/10G vo verzii staršej ako 1.15.5
RS720-E9-RS12-E vo verzii staršej ako 1.15.3
WS C621E SAGE vo verzii staršej ako 1.15.3
RS500A-E10-PS4 vo verzii staršej ako 1.15.3
RS500A-E10-RS4 vo verzii staršej ako 1.15.3
RS700A-E9-RS12V2 vo verzii staršej ako 1.15.3
RS700A-E9-RS4V2 vo verzii staršej ako 1.15.3
RS720A-E9-RS12V2 vo verzii staršej ako 1.15.3
RS720A-E9-RS24V2 vo verzii staršej ako 1.15.3
Z11PR-D16 vo verzii staršej ako 1.15.4

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.

Zdroje
https://exchange.xforce.ibmcloud.com/vulnerabilities/199454 https://www.twcert.org.tw/tw/cp-132-4574-b61a6-1.html https://www.asus.com/content/ASUS-Product-Security-Advisory/