BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 03. 2021 - 09. 03. 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-357

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 Apache

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na produkty Tomcat a Hive, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.03.2021

CVE

CVE-2020-1926, CVE-2021-25122, CVE-2021-25329

Zasiahnuté systémy

Apache Tomcat vo verzii staršej ako 7.0.108
Apache Tomcat vo verzii staršej ako 8.5.63
Apache Tomcat vo verzii staršej ako 9.0.43
Apache Tomcat vo verzii staršej ako 10.0.2
Apache Hive vo verzii staršej ako 2.3.8

Následky

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

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/197519
https://seclists.org/oss-sec/2021/q1/184
http://tomcat.apache.org/
https://exchange.xforce.ibmcloud.com/vulnerabilities/197515

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dve bezpečnostné zraniteľnosti v produkte Dell OpenManage Server Administrator

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoj produkt EMC OpenManage Server Administrator (OMSA), ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených požiadaviek získať administrátorský prístup do systému a následne prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.03.2021

CVE

CVE-2021-21513, CVE-2021-21514

Zasiahnuté systémy

Dell EMC OpenManage Server Administrator vo verzii staršej ako 9.4.0.3
Dell EMC OpenManage Server Administrator vo verzii staršej ako 9.5.0.1

Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom 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.dell.com/support/kbdoc/sk-sk/000183670/dsa-2021-040-dell-emc-openmanage-server-administrator-omsa-security-update-for-multiple-vulnerabilities
https://exchange.xforce.ibmcloud.com/vulnerabilities/197597

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte VMware View Planner

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt View Planner, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.03.2021

CVE

CVE-2021-21978

Zasiahnuté systémy

View Planner vo verzii staršej ako 4.6 Security Patch 1

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://www.vmware.com/security/advisories/VMSA-2021-0003.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/197669

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Salt Package Manager

Popis

Vývojári Salt Package Manager vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvoreného dopytu cez salt-api vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.03.2021

CVE

CVE-2021-25315

Zasiahnuté systémy

salt vo verzii staršej ako 3002.2-3
salt vo verzii staršej ako 3002.2-2.1

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://github.com/saltstack/salt-pack
https://software.opensuse.org/package/salt
https://bugzilla.suse.com/show_bug.cgi?id=1182382

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 ONLYOFFICE Document Server

Popis

Vývojári online kancelárskeho balíka ONLYOFFICE vydali bezpečnostnú aktualizáciu svojho produktu, 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

02.03.2021

CVE

CVE-2021-25829, CVE-2021-25830, CVE-2021-25831, CVE-2021-25832, CVE-2021-25833

Zasiahnuté systémy

ONLYOFFICE DocumentServer vo verzii staršej ako 6.2.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom 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/197570
https://github.com/ONLYOFFICE/DocumentServer

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 mymbCONNECT24 a mbCONNECT24

Popis

Spoločnosť MB connect line vydala bezpečnostné aktualizácie na produkty mbCONNECT24 a mymbCONNECT24, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.03.2021

CVE

CVE-2020-10384, CVE-2020-12527, CVE-2020-12528, CVE-2020-12529, CVE-2020-12530, CVE-2020-35557, CVE-2020-35558, CVE-2020-35559, CVE-2020-35560, CVE-2020-35561, CVE-2020-35563, CVE-2020-35564, CVE-2020-35565, CVE-2020-35566, CVE-2020-35567, CVE-2020-35568, CVE-2020-35569, CVE-2020-35570

Zasiahnuté systémy

mymbCONNECT24 vo verzii staršej ako 2.7.1
mbCONNECT24 vo verzii staršej ako 2.7.1

Následky

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

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://us-cert.cisa.gov/ics/advisories/icsa-21-061-03
https://mbconnectline.com/mymbconnect24-virtual/

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

Identifikátor

Viacero bezpečnostných zraniteľností v produkte GNU GRUB2

Popis

Vývojári zavádzača GRUB vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v implementácii rmmod a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.03.2021

CVE

CVE-2020-14372, CVE-2020-25632, CVE-2020-25647, CVE-2020-27749, CVE-2020-27779, CVE-2021-20225, CVE-2021-20233, CVE-2021-3418

Zasiahnuté systémy

GNU GRUB2
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://git.savannah.gnu.org/gitweb/?p=grub.git;a=shortlog;h=refs/heads/master

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://seclists.org/oss-sec/2021/q1/189
https://exchange.xforce.ibmcloud.com/vulnerabilities/197604
https://git.savannah.gnu.org/gitweb/?p=grub.git&view=view+git+repository

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

Identifikátor

Dve bezpečnostné zraniteľnosti v produktoch Rockwell Automation série 1734-AENTR

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na produkty série 1734-AENTR, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených HTTP požiadaviek vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.03.2021

CVE

CVE-2020-14502, CVE-2020-14504

Zasiahnuté systémy

1734-AENTR Series B s firmware vo verzii staršej ako 5.018
1734-AENTR Series C s firmware vo verzii staršej ako 6.013

Následky

Neoprávnená zmena v systéme

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-21-063-01

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Xerox AltaLink

Popis

Spoločnosť Xerox vydala bezpečnostné aktualizácie na produkty AltaLink, 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 požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.03.2021

CVE

CVE-2019-18629

Zasiahnuté systémy

Xerox AltaLink C8030 vo verzii staršej ako 101.001.099.28200
Xerox AltaLink C8035 vo verzii staršej ako 101.001.099.28200
Xerox AltaLink C8045 vo verzii staršej ako 101.002.099.28200
Xerox AltaLink C8055 vo verzii staršej ako 101.002.099.28200
Xerox AltaLink C8070 vo verzii staršej ako 101.003.099.28200
Xerox AltaLink B8045 vo verzii staršej ako 101.008.099.28200
Xerox AltaLink B8055 vo verzii staršej ako 101.008.099.28200
Xerox AltaLink B8065 vo verzii staršej ako 101.008.099.28200
Xerox AltaLink B8075 vo verzii staršej ako 101.008.099.28200

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/197743
https://securitydocs.business.xerox.com/wp-content/uploads/2021/03/cert_Security_Mini_Bulletin_XRX19AI_for_ALB80xx-C80xx_v1.1.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Cisco

Popis

Spoločnosť Cisco 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 vytvorených Ethernetových rámcov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.03.2021

CVE

CVE-2021-1285

Zasiahnuté systémy

1000 Series Integrated Services Routers (ISRs)
4000 Series Integrated Services Routers (ISRs)
Catalyst 8000V Edge Software
Catalyst 8200 Series Edge Platforms
Catalyst 8300 Series Edge Platforms
Cloud Services Router 1000V Series
Integrated Services Virtual Router (ISRv)
Presnú specifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n
https://exchange.xforce.ibmcloud.com/vulnerabilities/197685

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Endress Hauser

Popis

Spoločnosť Endress Hauser vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.03.2021

CVE

CVE-2020-12525

Zasiahnuté systémy

DeviceCare SFE100 vo verzii staršej ako 1.07.00 (vrátane)
Field Xpert SMTxx (Software SFE300) vo verzii staršej ako 1.05.00 (vrátane)
FieldCare SFE500 vo verzii staršej ako 2.15.01 (vrátane)
Asset Health Monitoring SRP700 (Software FieldCare SFE500) vo verzii staršej ako 2.15.01 (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.
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2021-005

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Schneider Electric

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného XML kódu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.03.2021

CVE

CVE-2020-28209, CVE-2020-28210, CVE-2020-7569, CVE-2020-7570, CVE-2020-7571, CVE-2020-7572, CVE-2020-7573

Zasiahnuté systémy

WebReports vo verzii staršej ako 3.2
WebStation vo verzii staršej ako 3.2
Enterprise Server installer vo verzii staršej ako 3.2
Enterprise Central installer vo verzii staršej ako 3.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom 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 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://us-cert.cisa.gov/ics/advisories/icsa-21-063-02
https://www.se.com/ww/en/download/document/SEVD-2020-315-04/