BEZPEČNOSTNÝ BULLETIN

Týždeň 19. 05. 2021 - 25. 05. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Cisco produkty - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	Pulse Connect Secure produkt - bezpečnostná zraniteľnosť	Vysoká	**8.5**
03.	Microsoft Windows JET Database Engine - bezpečnostná zraniteľnosť	Vysoká	**7.8**
04.	Trend Micro Maximum Security produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Emerson Rosemount X-STREAM Gas Analyzer - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
06.	Prometheus produkt - bezpečnostná zraniteľnosť	Vysoká	**7.4**
07.	BOSCH IndraMotion PLC produkty - bezpečnostná zraniteľnosť	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-430

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

Identifikátor

Cisco produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa, prostredníctvom zasielania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.05.2021

CVE

CVE-2021-1487, CVE-2021-1531

Zasiahnuté systémy

Cisco Prime Infrastructure vo verzii staršej ako 3.9
Cisco EPN Manager vo verzii staršej ako 5.1
Cisco Modeling Lab vo verzii staršej ako 2.2.1

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-cmd-inj-YU5e6tB3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB
https://tools.cisco.com/security/center/cvssCalculator.x?version=3.1&vector=CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Pulse Connect Secure produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Pulse Secure vydala bezpečnostnú aktualizáciu na produkt Pulse Connect Secure, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.05.2021

CVE

CVE-2021-22908

Zasiahnuté systémy

Pulse Connect Secure vo verzii staršej ako 9.1R11.5

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://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800

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

Identifikátor

Microsoft Windows JET Database Engine - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Microsoft Windows JET Database Engine.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.05.2021

CVE

-

Zasiahnuté systémy

Microsoft Windows JET Database Engine všetky verzie

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

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-21-594/
https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-jet-database-engine-could-allow-for-arbitrary-code-execution_2021-069/

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

Identifikátor

Trend Micro Maximum Security produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Maximum Security, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.05.2021

CVE

CVE-2021-32460

Zasiahnuté systémy

Maximum Security vo verzii staršej ako May 20, 2021

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

Zdroje

https://helpcenter.trendmicro.com/en-us/article/TMKA-10336
https://www.zerodayinitiative.com/advisories/ZDI-21-603/

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

Identifikátor

Emerson Rosemount X-STREAM Gas Analyzer - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Emerson Rosemount vydala bezpečnostnú aktualizáciu na svoj produkt X-STREAM Gas Analyzer, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

18.05.2021

CVE

CVE-2021-27457, CVE-2021-27459, CVE-2021-27461, CVE-2021-27463, CVE-2021-27465, CVE-2021-27467

Zasiahnuté systémy

X-STREAM enhanced XEGP všetky verzie
X-STREAM enhanced XEGK všetky verzie
X-STREAM enhanced XEFD všetky verzie
X-STREAM enhanced XEXF všetky verzie
Presné informácie ohľadom aktualizácie firmwaru získate na emailovej adrese:
TechSupport.Hasselroth@emerson.com

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-138-01

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

Identifikátor

Prometheus produkt - bezpečnostná zraniteľnosť

Popis

Vývojári programu Prometheus 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 vytvorenej URL vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.05.2021

CVE

CVE-2021-29622

Zasiahnuté systémy

Prometheus vo verzii staršej ako 2.26.1
Prometheus vo verzii staršej ako 2.27.1

Následky

Neoprávnená zmena v systéme

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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/202131
https://github.com/prometheus/prometheus
https://seclists.org/oss-sec/2021/q2/156

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

Identifikátor

BOSCH IndraMotion PLC produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť BOSCH vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.05.2021

CVE

CVE-2021-29242

Zasiahnuté systémy

Rexroth IndraMotion MLC
Rexroth IndraMotion MLD
Rexroth IndraMotion MTX
ctrlX CORE PLC App Release vo verzii staršej ako 01V10

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-350374.html
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=
https://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911342562