BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 04. 2022 - 19. 04. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Valmet DNA produkt - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Microsoft Edge - bezpečnostná zraniteľnosť	Vysoká	**8.3**
03.	Johnson Controls Metasys ADS/ADX/OAS servery - bezpečnostná zraniteľnosť	Vysoká	**8.1**
04.	LDAP Account Manager (LAM) - bezpečnostná zraniteľnosť	Vysoká	**8.1**
05.	Siemens produkty - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
06.	Inductive Automation Ignition produkt - bezpečnostná zraniteľnosť	Vysoká	**7.0**

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:
01794/2022/SK-CERT-737

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

Identifikátor

Valmet DNA produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Valmet vydala bezpečnostnú aktualizáciu na produkt DNA, ktorá opravuje 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 paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.04.2022

CVE

CVE-2021-26726

Zasiahnuté systémy

Valmet DNA vo verzii staršej ako Collection 2022

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-102-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na produkt Microsoft Edge, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.04.2022

CVE

CVE-2022-29144

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 100.0.1185.44

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29144
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29144
https://exchange.xforce.ibmcloud.com/vulnerabilities/224528

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

Identifikátor

Johnson Controls Metasys ADS/ADX/OAS servery - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na servery Metasys ADS/ADX/OAS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.04.2022

CVE

CVE-2021-36205

Zasiahnuté systémy

All Metasys ADS/ADX/OAS Servers: Versions 10 and 11

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-104-02

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

Identifikátor

LDAP Account Manager (LAM) - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja LDAP Account Manager vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.04.2022

CVE

CVE-2022-24851

Zasiahnuté systémy

LDAP Account Manager (LAM) vo verzii staršej ako 7.9.1

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://github.com/LDAPAccountManager/lam/security/advisories/GHSA-f2fr-cccr-583v
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24851
https://exchange.xforce.ibmcloud.com/vulnerabilities/224515

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

Identifikátor

Siemens produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.04.2022

CVE

CVE-2021-40368, CVE-2022-27194

Zasiahnuté systémy

SIMATIC S7-400 HV6 vo verzii staršej ako v6.0.10
SIMATIC S7-400 PN/DP V7 všetky verzie
SIMATIC S7-410 V8 všetky verzie
SIMATIC S7-410 V10 vo verzii staršej ako v10.1
SIMATICS PCS neo (Administration Console) vo verzii staršej ako v3.1 SP1
SINETPLAN všetky verzie
TIA Portal verzie 15, 15.1, 16 a 17

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade produktov, pre ktoré ešte neboli vydané aktualizácie, odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Pre dočasnú mitigáciu v prípade produktov SIMATICS PCS neo, SINETPLAN a TIA Portal odporúča výrobca obmedziť prístup k portu 8888/tcp na localhost.
V prípade produktov SIMATIC S7-400 PN/DP V7 a SIMATIC S7-410 V8 odporúča výrobca ako dočasnú mitigáciu obmedziť prístup k portu 102/tcp iba na dôveryhodných používateľov a systémy.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-22-104-16
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-12
https://cert-portal.siemens.com/productcert/pdf/ssa-711829.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-557541.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Inductive Automation Ignition produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Inductive Automation vydala bezpečnostnú aktualizáciu na produkt Ignition, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

13.04.2022

CVE

CVE-2022-1264

Zasiahnuté systémy

Inductive Automation Ignition vo verzii staršej ako 8.1.10

Následky

Neoprávnená zmena v systéme

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-22-102-03