BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 09. 2021 - 16. 09. 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-549

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

Identifikátor

Cisco IOS XR - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoj produkt IOS XR, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.09.2021

CVE

CVE-2021-1440, CVE-2021-34708, CVE-2021-34709, CVE-2021-34713, CVE-2021-34718, CVE-2021-34719, CVE-2021-34720, CVE-2021-34721, CVE-2021-34722, CVE-2021-34728, CVE-2021-34737, CVE-2021-34771, CVE-2021-34785, CVE-2021-34786

Zasiahnuté systémy

Cisco IOS XR
Presný zoznam zraniteľných verzií sa nachádza na webovej adrese: https://tools.cisco.com/security/center/publicationListing.x

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npspin-QYpwdhFD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsla-ZA3SRrpP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-scp-inject-QwZOCv2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privescal-dZYMrKf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrbgp-rpki-dos-gvmjqxbk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lnt-QN9mCzwn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-infodisc-CjLdGMc5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-pjPVReLU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-cmd-inj-wbZKvPxc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-dJ9JT67N
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npspin-QYpwdhFD

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

Identifikátor

HAProxy - bezpečnostná zraniteľnosť

Popis

Vývojári softvérových riešení HAProxy vydali bezpečnostné aktualizácie na viacero svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

07.09.2021

CVE

CVE-2021-40346

Zasiahnuté systémy

HAProxy 2.0 vo verzii staršej ako 2.0.25
HAProxy 2.2 vo verzii staršej ako 2.2.17
HAProxy 2.3 vo verzii staršej ako 2.3.14
HAProxy 2.4 vo verzii staršej ako 2.4.4
HAProxy Enterprise 2.0r1 vo verzii staršej ako 2.0r1-235.1230
HAProxy Enterprise 2.1r1 vo verzii staršej ako 2.1r1-238.625
HAProxy Enterprise 2.2r1 vo verzii staršej ako 2.2r1-241.505
HAProxy Enterprise 2.3r1 vo verzii staršej ako 2.3r1-242.345
HAProxy Kubernetes Ingress Controller 1.6 vo verzii staršej ako 1.6.7
HAProxy Enterprise Kubernetes Ingress Controller 1.6 vo verzii staršej ako 1.6.7
HAProxy ALOHA 11.5 vo verzii staršej ako 11.5.13
HAProxy ALOHA 12.5 vo verzii staršej ako 12.5.5
HAProxy ALOHA 13.0 vo verzii staršej ako 13.0.7

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.haproxy.com/blog/september-2021-duplicate-content-length-header-fixed/
https://jfrog.com/blog/critical-vulnerability-in-haproxy-cve-2021-40346-integer-overflow-enables-http-smuggling/
https://www.securityweek.com/haproxy-vulnerability-leads-http-request-smuggling
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

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

Identifikátor

Node.js tar a @npmcli/arborist - viacero bezpečnostných zraniteľností

Popis

Vývojári knižníc node-tar a @npmcli/arborist vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšia zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom vytvárania alebo prepisovania systémových súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

08.09.2021

CVE

CVE-2021-32803, CVE-2021-32804, CVE-2021-37701, CVE-2021-37712, CVE-2021-37713, CVE-2021-39134, CVE-2021-39135

Zasiahnuté systémy

@npmcli/arborist vo verzii staršej ako 2.8.2
Node-tar 3.2.3
Node-tar 4.4.19
Node-tar 5.0.11
Node-tar 6.1.10

Následky

Vykonanie škodlivého kódu
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.blog/2021-09-08-github-security-update-vulnerabilities-tar-npmcli-arborist/
https://www.securityweek.com/github-patches-security-flaws-core-nodejs-dependencies
https://www.bleepingcomputer.com/news/security/github-finds-7-code-execution-vulnerabilities-in-tar-and-npm-cli/

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

Identifikátor

Sensormatic Electronics kamerové systémy Illustra - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostné aktualizácie na kamerové systémy Illustra, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.09.2021

CVE

CVE-2021-3156

Zasiahnuté systémy

Pro Gen 3 vo verzii staršej ako 2.8.0
Flex Gen 2 vo verzii staršej ako 1.9.4
Pro 2 (všetky verzie - ukončená podpora)
Insight vo verzii staršej ako 1.4.0

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-245-01

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

Identifikátor

Delta Electronics DOPSoft 2 produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na produkt DOPSoft 2, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvoreného súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.09.2021

CVE

CVE-2021-38402, CVE-2021-38404, CVE-2021-38406

Zasiahnuté systémy

DOPSoft 2 vo verzii staršej ako 2.00.07 (vrátane - ukončená podpora)

Následky

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

Odporúčania

Výrobca odporúča používateľom, aby prešli na alternatívny softvér, nakoľko produktu DOPSoft 2 bola ukončená podpora.
Ďalej výrobca odporúča používať iba projektové súbory z dôveryhodných zdrojov.
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).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-252-02

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

Identifikátor

Mitsubishi Electric MELSEC iQ-R séria CPU modulov - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na MELSEC iQ-R sériu CPU modulov, 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 a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

07.09.2021

CVE

CVE-2021-20594, CVE-2021-20597, CVE-2021-20598

Zasiahnuté systémy

R08/16/32/120SFCPU všetky verzie
R08/16/32/120PSFCPU všetky verzie

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Až do vydania bezpečnostnej aktualizácie odporúča výrobca zapnúť funkciu filtra IP adries podľa postupu uvedeného na webovej adrese:
https://www.mitsubishifa.co.th/files/dl/plc/sh081257eng/sh081257engs.pdf
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-21-250-01
https://www.mitsubishifa.co.th/files/dl/plc/sh081257eng/sh081257engs.pdf

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

Identifikátor

AVEVA Platform Common Services (PCS) Portal - bezpečnostná zraniteľnosť

Popis

Spoločnosť AVEVA vydala bezpečnostnú aktualizáciu na produkt PCS Portal, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom povrhnutia špeciálne vytvorenej DLL, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.09.2021

CVE

CVE-2021-38410

Zasiahnuté systémy

AVEVA PCS vo verzii staršej ako 4.5.3
AVEVA PCS vo verzii staršej ako 4.4.7

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-252-01
https://www.aveva.com/en/support-and-success/cyber-security-updates/