BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 06. 2021 - 22. 06. 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-456

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

Identifikátor

Schneider Electric Enerlin'X Com'X 510 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na produkt Enerlin'X Com'X 510, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

18.06.2021

CVE

CVE-2021-22769

Zasiahnuté systémy

Enerlin'X Com'X 510 vo verzii staršej ako v6.8.4

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Eskalácia privilégií

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-21-168-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NVIDIA Jetson produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom pretečenia zásobníka, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.06.2021

CVE

-

Zasiahnuté systémy

Jetson TX1 vo verzii staršej ako 32.5.1 Debian update
Jetson TX2 vo verzii staršej ako 32.5.1 Debian update
Jetson TX2 NX vo verzii staršej ako 32.5.1 Debian update
Jetson AGX Xavier vo verzii staršej ako 32.5.1 Debian update
Jetson Xavier NX vo verzii staršej ako 32.5.1 Debian update
Jetson Nano vo verzii staršej ako 32.5.1 Debian update
Jetson Nano 2GB vo verzii staršej ako 32.5.1 Debian update

Následky

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

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://nvidia.custhelp.com/app/answers/detail/a_id/5205

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

Identifikátor

Palo Alto Networks Cortex XDR Agent - bezpečnostná zraniteľnosť

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostnú aktualizáciu na svoj produkt Cortex XDR Agent, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.06.2021

CVE

CVE-2021-3041

Zasiahnuté systémy

Cortex XDR Agent vo verzii staršej ako 7.2.3 - 171
Cortex XDR Agent vo verzii staršej ako 6.1.8
Cortex XDR Agent vo verzii staršej ako 5.0.11

Následky

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

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).
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://security.paloaltonetworks.com/CVE-2021-3041

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

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.06.2021

CVE

CVE-2021-1134, CVE-2021-1395, CVE-2021-1524, CVE-2021-1541, CVE-2021-1542, CVE-2021-1543, CVE-2021-1566, CVE-2021-1567, CVE-2021-1568, CVE-2021-1571

Zasiahnuté systémy

Cisco Small Business 220 Series Smart Switches s firmware vo verzii staršej ako 1.2.0.6
Cisco Email Security Appliance vo verzii staršej ako 12.5.3-035
Cisco Email Security Appliance vo verzii staršej ako 13.0.0-030
Cisco Email Security Appliance vo verzii staršej ako 13.5.3-010
Cisco Web Security Appliance vo verzii staršej ako 11.8.3-021
Cisco Web Security Appliance vo verzii staršej ako 12.0.3-005
Cisco Web Security Appliance vo verzii staršej ako 12.5.1-043
Cisco DNA Center Software vo verzii staršej ako 2.2.2.3
Cisco AnyConnect Secure Mobility Client pre Windows vo verzii staršej ako 4.10.01075

Následky

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-cert-vali-n8L97RW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-certvalid-USEj2CZk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-pos-dll-ff8j6dFv

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

Identifikátor

Softing OPC-UA C++ SDK - bezpečnostná zraniteľnosť

Popis

Spoločnosť Softing vydala bezpečnostnú aktualizáciu na produkt OPC-UA C++ SDK, ktorá opravuje bezpečnostnú zraniteľnosť.
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

18.06.2021

CVE

CVE-2021-32994

Zasiahnuté systémy

OPC UA C++ SDK vo verzii staršej ako 5.65

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-168-02

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

Identifikátor

Advantech WebAccess/SCADA produkt - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na produkt WebAccess/SCADA, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.06.2021

CVE

CVE-2021-32954, CVE-2021-32956

Zasiahnuté systémy

WebAccess/SCADA Versions vo verzii staršej ako 9.0.1

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://us-cert.cisa.gov/ics/advisories/icsa-21-168-03