BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 10. 2021 - 19. 10. 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-594

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

Identifikátor

Zoho ManageEngine ADManager Plus produkt - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoho vydala bezpečnostnú aktualizáciu na produkt ManageEngine ADManager Plus, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.10.2021

CVE

CVE-2021-20130, CVE-2021-20131

Zasiahnuté systémy

Zoho ManageEngine ADManager Plus vo verzii staršej ako 7113

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://www.tenable.com/security/research/tra-2021-43
https://www.manageengine.com/products/ad-manager/release-notes.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20130
https://exchange.xforce.ibmcloud.com/vulnerabilities/211252

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-594

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári software Linux Kernel vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.10.2021

CVE

CVE-2021-34866

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.13

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.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-21-1148/
https://www.kernel.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34866
https://exchange.xforce.ibmcloud.com/vulnerabilities/211255

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

Identifikátor

Siemens produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens 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 s právomocami používateľa vykonať zmeny v systéme a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.10.2021

CVE

CVE-2017-2680, CVE-2017-2681, CVE-2019-10923, CVE-2019-10936, CVE-2019-13946, CVE-2020-28400, CVE-2021-33722, CVE-2021-33723, CVE-2021-33724, CVE-2021-33725, CVE-2021-33726, CVE-2021-33727, CVE-2021-33728, CVE-2021-33729, CVE-2021-33730, CVE-2021-33731, CVE-2021-33732, CVE-2021-33733, CVE-2021-33734, CVE-2021-33735, CVE-2021-33736, CVE-2021-37199, CVE-2021-37202, CVE-2021-37203, CVE-2021-37206, CVE-2021-41533, CVE-2021-41534, CVE-2021-41535, CVE-2021-41536, CVE-2021-41537, CVE-2021-41538, CVE-2021-41539, CVE-2021-41540, CVE-2021-41546

Zasiahnuté systémy

Siemens RUGGEDCOM ROX
Siemens RUGGEDCOM ROX Devices
Siemens SINEC NMS
Siemens SINUMERIK
Siemens Solid Edge
Siemens SIPROTEC 5
Siemens Linux-based Products
Siemens Industrial Real-Time (IRT) Devices
Siemens SCALANCE X
Siemens Industrial Products
Siemens PROFINET DCP
Siemens PROFINET-IO Stack
Siemens PROFINET Devices
Všetky zasiahnuté verzie, ich aktuálne verzie a mitigácie sú dostupné na webových adresách uvedených medzi zdrojmi.

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému Zneprístupnenie služby Eskalácia privilégií Neoprávnená zmena v systéme Neoprávnený prístup k citlivým informáciám

Odporúčania
Administrátorom a používateľom odporúčame bezodkladne 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-21-259-01 https://us-cert.cisa.gov/ics/advisories/icsa-21-287-05 https://us-cert.cisa.gov/ics/advisories/icsa-21-287-04 https://us-cert.cisa.gov/ics/advisories/icsa-21-287-06 https://us-cert.cisa.gov/ics/advisories/icsa-21-287-08 https://us-cert.cisa.gov/ics/advisories/icsa-21-257-16 https://us-cert.cisa.gov/ics/advisories/icsa-21-194-03 https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04 https://us-cert.cisa.gov/ics/advisories/icsa-19-283-01 https://us-cert.cisa.gov/ics/advisories/ICSA-19-085-01 https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01 https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

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

Identifikátor

Schneider Electric ConneXium Network Manager (CNM) - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na produkt ConneXium Network Manager (CNM) Software, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorenej webovej stránky, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.10.2021

CVE

CVE-2021-22801

Zasiahnuté systémy

ConneXium Network Manager (všetky verzie)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame postupovať podľa odporúčaní výrobcu zverejnených na https://us-cert.cisa.gov/ics/advisories/icsa-21-287-01
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics
https://us-cert.cisa.gov/reportCISA
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-01

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

Identifikátor

Foxit PDF Reader, Foxit PDF Editor - bezpečnostné zraniteľnosti

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na produkty Foxit PDF Reader a Foxit PDF Editor pre MAC a Windows, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.10.2021

CVE

CVE-2021-40326, CVE-2021-41780, CVE-2021-41781, CVE-2021-41782, CVE-2021-41783, CVE-2021-41784, CVE-2021-41785

Zasiahnuté systémy

Foxit PDF Reader (starší názov - Foxit Reader) vo verzii staršej ako 11.0.1.49938
Foxit PDF Editor (starší názov - Foxit PhantomPDF) vo verzii staršej ako 11.0.1.49938
Foxit PDF Editor (starší názov - Foxit PhantomPDF) vo verzii staršej ako 11.0.0.49893
Foxit PDF Editor (starší názov - Foxit PhantomPDF) vo verzii staršej ako 10.1.5.37672
Foxit PDF Reader Mac (starší názov - Foxit Reader Mac) vo verzii staršej ako 11.0.1.0719
Foxit PDF Editor Mac (starší názov - Foxit PhantomPDF Mac) vo verzii staršej ako 11.0.1.0719

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.

Zdroje

https://www.foxit.com/support/security-bulletins.html
https://www.zerodayinitiative.com/advisories/published/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41783
https://www.cybersecurity-help.cz/vdb/SB2021101204

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-594