BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 11. 2021 - 16. 11. 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-618

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

Identifikátor

Schneider Electric GUIcon produkt - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu GUIcon od spoločnosti Schneider Electric.
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

09.11.2021

CVE

CVE-2021-22807, CVE-2021-22808, CVE-2021-22809

Zasiahnuté systémy

GUIcon vo verzii staršej ako 2.0 (Build 683.003) (vrátane - ukončená podpora)

Následky

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

Odporúčania

Podpora nástroja GUIcon bola ukončená 24.6.2020, z toho dôvodu nie je k dispozícii jeho aktualizovaná verzia.
Podľa výrobcu existuje jediný spôsob akým môže útočník zneužiť uvedené zraniteľnosti a to prostredníctvom podvrhnutia škodlivého konfiguračného súboru GUIcon *.gd1.
Z toho dôvodu odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Vzhľadom k tomu, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
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://us-cert.cisa.gov/ics/advisories/icsa-21-313-02
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-313-07

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

Identifikátor

Citrix produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Citrix vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.11.2021

CVE

CVE-2021-22955, CVE-2021-22956

Zasiahnuté systémy

Citrix ADC a Citrix Gateway vo verzii staršej ako 13.1-4.43
Citrix ADC a Citrix Gateway vo verzii staršej ako 12.1-63.22
Citrix ADC a NetScaler Gateway vo verzii staršej ako 11.1-65.23
Citrix ADC 12.1-FIPS vo verzii staršej ako 12.1-55.257
Citrix SD-WAN WANOP Edition vo verzii staršej ako 11.4.2
Citrix SD-WAN WANOP Edition vo verzii staršej ako 10.2.9c

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.citrix.com/article/CTX330728
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22955
https://exchange.xforce.ibmcloud.com/vulnerabilities/213066
https://threatpost.com/critical-citrix-bug-etwork-cloud-app-access/176183/
https://www.securityweek.com/citrix-patches-critical-vulnerability-adc-gateway

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

Identifikátor

VISAM VBASE produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VISAM vydala bezpečnostnú aktualizáciu na produkt VBASE, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.11.2021

CVE

CVE-2005-2475, CVE-2018-14333, CVE-2018-16550, CVE-2019-18988, CVE-2020-13699, CVE-2021-34803, CVE-2021-38417, CVE-2021-42535, CVE-2021-42537

Zasiahnuté systémy

VBASE vo verzii staršej ako v11.7.0.2

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.
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/advisories/icsa-21-308-01

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

Identifikátor

mySCADA myDESIGNER - bezpečnostná zraniteľnosť

Popis

Spoločnosť mySCADA vydala bezpečnostnú aktualizáciu na produkt myDESIGNER, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.11.2021

CVE

CVE-2021-43555

Zasiahnuté systémy

myDESIGNER vo verzii staršej ako 8.22.0

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.
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-21-313-04

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel procesory - bezpečnostná zraniteľnosť

Popis

Spoločnosť Intel vydala bezpečnostnú aktualizáciu na svoje portfólio procesorov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.11.2021

CVE

CVE-2021-0146

Zasiahnuté systémy

Intel Pentium Processor J Series, N Series
Intel Celeron Processor J Series, N Series
Intel Atom Processor A Series
Intel Atom Processor E3900 Series
Intel Pentium Processor Silver Series/ J&N Series
Intel Atom Processor C3000
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html

Následky

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie. 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. V prípade, že prevádzkujete fyzické servery s operačným systémom Linux, uistite sa, že máte nainštalovaný balík intel-microcode. Na BSD systémoch môžete použiť balík cpupdate. Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html https://twitter.com/_markel___/status/1458147735270481926?t=T7ZGXJ6YOAXOv61wQWE6PA&s=19 https://threatpost.com/intel-processor-bug-encryption-keys/176355/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware vCenter Server - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu vCenter Server od spoločnosti VMware.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.11.2021

CVE

CVE-2021-22048

Zasiahnuté systémy

vCenter Server vo verzii staršej ako 7.0 (vrátane)
vCenter Server vo verzii staršej ako 6.7 (vrátane)
vCenter Server vo verzii staršej ako 6.5 (vrátane)
Cloud Foundation (vCenter Server) vo verzii staršej ako 4.x (vrátane)
Cloud Foundation (vCenter Server) vo verzii staršej ako 3.x (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.vmware.com/security/advisories/VMSA-2021-0025.html
https://www.securityweek.com/vmware-working-patches-serious-vcenter-server-vulnerability