BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 08. 2021 - 24. 08. 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-527

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

Identifikátor

AVEVA SuiteLink Server - viacero bezpečnostných zraniteľností

Popis

Spoločnosť AVEVA Software vydala bezpečnostnú aktualizáciu na produkt SuiteLink Server, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia 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

19.08.2021

CVE

CVE-2021-32959, CVE-2021-32963, CVE-2021-32971, CVE-2021-32979, CVE-2021-32987, CVE-2021-32999

Zasiahnuté systémy

AVEVA SuiteLink Server vo verzii staršej ako 3.2.002
AVEVA Communication Drivers Pack vo verzii staršej ako 2020 R2.1
AVEVA MES vo verzii staršej ako 2014 R3

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://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/SecurityBulletin_AVEVA-2021-003.pdf
https://us-cert.cisa.gov/ics/advisories/icsa-21-231-01

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

Identifikátor

Adobe Photoshop - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Photoshop, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.08.2021

CVE

CVE-2021-36065, CVE-2021-36066

Zasiahnuté systémy

Photoshop 2020 vo verzii staršej ako 21.2.11
Photoshop 2021 vo verzii staršej ako 22.5

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).

Zdroje

https://helpx.adobe.com/security/products/photoshop/apsb21-68.html
https://www.securityweek.com/adobe-plugs-critical-photoshop-security-flaws

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

Identifikátor

Razer Synapse - zero day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zero day bezpečnostnej zraniteľnosti produktu Razer Synapse.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

24.08.2021

CVE

-

Zasiahnuté systémy

Razer Synapse vo verzii staršej ako 2.0 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www.cybersafe.news/razer-bug-allows-attackers-to-take-over-windows-pcs/
https://streamable.com/e/q2dsji

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

Identifikátor

Siemens SINEMA Remote Connect Client - bezpečnostná zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na produkt Sinema Remote Connect Client, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.08.2021

CVE

CVE-2021-31338

Zasiahnuté systémy

Siemens Sinema Remote Connect Client vo verzii staršej ako V3.0 SP1

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-816035.pdf
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31338
https://exchange.xforce.ibmcloud.com/vulnerabilities/207887

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Baserow produkt- bezpečnostná zraniteľnosť

Popis

Vývojári aplikácie Baserow vydali bezpečnostnú aktualizáciu svojho produktu, 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, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

20.08.2021

CVE

CVE-2021-22255

Zasiahnuté systémy

Baserow vo verzii staršej ako 1.0.0

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.

Zdroje

https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22255.json
https://baserow.io/blog/march-2021-release-of-baserow
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22255
https://exchange.xforce.ibmcloud.com/vulnerabilities/207955

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

Identifikátor

Juniper Networks Junos OS - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Juniper Networks vydala bezpečnostné aktualizácie na produkt Junos OS, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.08.2021

CVE

CVE-2021-0283, CVE-2021-0284

Zasiahnuté systémy

Junos OS vo verzii staršej ako 12.3R12-S19;
Junos OS vo verzii staršej ako 15.1R7-S10;
Junos OS vo verzii staršej ako 17.3R3-S12;
Junos OS vo verzii staršej ako 18.4R3-S9;
Junos OS vo verzii staršej ako 19.1R3-S7;
Junos OS vo verzii staršej ako 19.2R1-S7,
Junos OS vo verzii staršej ako 19.2R3-S3;
Junos OS vo verzii staršej ako to 19.3R3-S3;
Junos OS vo verzii staršej ako to 19.4R3-S5;
Junos OS vo verzii staršej ako 20.1R3-S1;
Junos OS vo verzii staršej ako 20.2R3-S2;
Junos OS vo verzii staršej ako 20.3R3-S1;
Junos OS vo verzii staršej ako 20.4R2-S2,
Junos OS vo verzii staršej ako 20.4R3;
Junos OS vo verzii staršej ako 21.1R2;
Junos OS vo verzii staršej ako 21.2R2.

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11200&cat=SIRT_1&actp=LIST

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

Identifikátor

Cerber Tech plugin pre WordPress - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu Cerber Tech vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.08.2021

CVE

CVE-2021-37597

Zasiahnuté systémy

Cerber Tech WP Cerber plugin vo verzii staršej ako 8.9.3

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/fireeye/Vulnerability-Disclosures/blob/master/FEYE-2021-0023/FEYE-2021-0023.md
https://wpcerber.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37597
https://exchange.xforce.ibmcloud.com/vulnerabilities/207934

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

Identifikátor

Mozilla Firefox a Thunderbird - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkty Firefox a Thunderbird, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.08.2021

CVE

CVE-2021-29991

Zasiahnuté systémy

Firefox vo verzii staršej ako 91.0.1
Thunderbird vo verzii staršej ako 91.0.1

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/
https://access.redhat.com/security/cve/cve-2021-29991