BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 09. 2021 - 28. 09. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Amazon AWS WorkSpaces client - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Netgear produkty - bezpečnostná zraniteľnosť	Vysoká	**8.1**
03.	Trane Symbio produkty - bezpečnostná zraniteľnosť	Vysoká	**7.5**
04.	Sparkle Motion Nokogiri - bezpečnostná zraniteľnosť	Vysoká	**7.5**
05.	OpenSSH - bezpečnostná zraniteľnosť	Vysoká	**7.4**
06.	Trend Micro HouseCall produkt - bezpečnostná zraniteľnosť	Vysoká	**7.3**

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-570

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

Identifikátor

Amazon AWS WorkSpaces client - bezpečnostná zraniteľnosť

Popis

Spoločnosť Amazon vydala bezpečnostnú aktualizáciu na produkt AWS WorkSpaces client, ktorá opravuje bezpečnostnú zraniteľnosť. 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

21.09.2021

CVE

CVE-2021-38112

Zasiahnuté systémy

Amazon AWS WorkSpaces client vo verzii staršej ako 3.1.9

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://rhinosecuritylabs.com/aws/cve-2021-38112-aws-workspaces-rce/
https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-windows-client.html#windows-release-notes
https://www.securityweek.com/remote-code-execution-vulnerability-found-aws-workspaces
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38112
https://exchange.xforce.ibmcloud.com/vulnerabilities/209922

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-570

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

Identifikátor

Netgear produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Netgear vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.09.2021

CVE

CVE-2021-40847

Zasiahnuté systémy

R6400v2 s firmware vo verzii staršej ako 1.0.4.120
R6700 s firmware vo verzii staršej ako 1.0.2.26
R6700v3 s firmware vo verzii staršej ako 1.0.4.120
R6900 s firmware vo verzii staršej ako 1.0.2.26
R6900P s firmware vo verzii staršej ako 3.3.142_HOTFIX
R7000 s firmware vo verzii staršej ako 1.0.11.128
R7000P s firmware vo verzii staršej ako 1.3.3.142_HOTFIX
R7850 s firmware vo verzii staršej ako 1.0.5.76
R7900 s firmware vo verzii staršej ako 1.0.4.46
R8000 s firmware vo verzii staršej ako 1.0.4.76
RS400 s firmware vo verzii staršej ako 1.5.1.80

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://kb.netgear.com/000064039/Security-Advisory-for-Remote-Code-Execution-on-Some-Routers-PSV-2021-0204
https://threatpost.com/netgear-soho-security-bug-rce/174921/
https://blog.grimm-co.com/2021/09/mama-always-told-me-not-to-trust.html
https://thehackernews.com/2021/09/high-severity-rce-flaw-disclosed-in.html

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

Identifikátor

Trane Symbio produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trane vydala bezpečnostné aktualizácie na produkty Symbio, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.09.2021

CVE

CVE-2021-38448

Zasiahnuté systémy

Symbio 700 controller vo verzii staršej ako v1.00.0023
Symbio 800 controller vo verzii staršej ako v1.00.0007

Následky

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

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01

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

Identifikátor

Sparkle Motion Nokogiri - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice Sparkle Motion Nokogiri vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvoreného XML dokumentu, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

27.09.2021

CVE

CVE-2021-41098

Zasiahnuté systémy

Sparkle Motion Nokogiri vo verzii staršej ako 1.12.5

Následky

Neoprávnený prístup k citlivým údajom

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 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://github.com/sparklemotion/nokogiri/security/advisories/GHSA-2rr5-8q37-2w7h
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41098
https://exchange.xforce.ibmcloud.com/vulnerabilities/210112

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

Identifikátor

OpenSSH - bezpečnostná zraniteľnosť

Popis

Vývojári sady nástrojov OpenSSH vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.09.2021

CVE

CVE-2021-41617

Zasiahnuté systémy

OpenBSD OpenSSH vo verzii staršej ako 8.8

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://www.openwall.com/lists/oss-security/2021/09/26/1
https://www.openssh.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41617
https://exchange.xforce.ibmcloud.com/vulnerabilities/210062

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

Identifikátor

Trend Micro HouseCall produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trend Micro HouseCall for Home Networks privilege escalation vydala bezpečnostnú aktualizáciu na produkt HouseCall, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom povrhnutia špeciálne vytvorených súborov, eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.09.2021

CVE

CVE-2021-32466

Zasiahnuté systémy

Trend Micro HouseCall vo verzii staršej ako 5.3.1285

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.
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://www.zerodayinitiative.com/advisories/ZDI-21-1112/
https://helpcenter.trendmicro.com/en-us/article/tmka-10626
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32466
https://exchange.xforce.ibmcloud.com/vulnerabilities/210050