BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 12. 2021 - 05. 01. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Netgear Nighthawk RAX43 - bezpečnostná zraniteľnosť	Vysoká	**8.4**
02.	Gif2apng produkt - bezpečnostná zraniteľnosť	Vysoká	**7.8**
03.	Zyxel séria GS1900 - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
04.	Mermaid - bezpečnostná zraniteľnosť	Vysoká	**7.2**
05.	SuiteCRM - bezpečnostná zraniteľnosť	Vysoká	**7.2**
06.	Bitmask Riseup VPN produkt - bezpečnostná zraniteľnosť	Vysoká	**7.0**

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-649

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Netgear Nighthawk RAX43 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Netgear vydala bezpečnostnú aktualizáciu na produkt Nighthawk RAX, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.12.2021

CVE

CVE-2021-20168

Zasiahnuté systémy

Netgear Nighthawk RAX43

Následky

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

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.netgear.com/home/wifi/routers/rax43/
https://www.tenable.com/security/research/tra-2021-55
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20168
https://exchange.xforce.ibmcloud.com/vulnerabilities/216413

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-649

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

Identifikátor

Gif2apng produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Gif2apng.
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

27.12.2021

CVE

CVE-2021-45911

Zasiahnuté systémy

gif2apng vo verzii staršej ako 1.9 (vrátane)

Následky

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

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.
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://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1002687
http://gif2apng.sourceforge.net
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45911
https://exchange.xforce.ibmcloud.com/vulnerabilities/216231

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

Identifikátor

Zyxel séria GS1900 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu na sériu produktov GS1900 a XGS, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.12.2021

CVE

CVE-2021-35031, CVE-2021-35032

Zasiahnuté systémy

GS1900-8 vo verzii staršej ako V2.70(AAHH.0)C0 Nov. 2021
GS1900-8HP vo verzii staršej ako V2.70(AAHI.0)C0 Nov. 2021
GS1900-10HP vo verzii staršej ako V2.70(AAZI.0)C0 Nov. 2021
GS1900-16 vo verzii staršej ako V2.70(AAHJ.0)C0 Nov. 2021
GS1900-24E vo verzii staršej ako V2.70(AAHK.0)C0 Nov. 2021
GS1900-24EP vo verzii staršej ako V2.70(ABTO.0)C0 Nov. 2021
GS1900-24 vo verzii staršej ako V2.70(AAHL.0)C0 Nov. 2021
GS1900-24HP vo verzii staršej ako V2.70(AAHM.0)C0 Nov. 2021
GS1900-24HPv2 vo verzii staršej ako V2.70(ABTP.0)C0 Nov. 2021
GS1900-48 vo verzii staršej ako V2.70(AAHN.0)C0 Nov. 2021
GS1900-48HP vo verzii staršej ako V2.70(AAHO.0)C0 Nov. 2021
GS1900-48HPv2 vo verzii staršej ako V2.70(ABTQ.0)C0 Nov. 2021
XGS1210-12 vo verzii staršej ako V1.00(ABTY.5)C0 Dec. 2021
XGS1250-12 vo verzii staršej ako V1.00(ABWE.1)C0 Dec. 2021

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

Zdroje
https://www.zyxel.com/support/Zyxel_security_advisory_for_OS_command_injection_vulnerabilities_of_switches.shtml http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35032 https://exchange.xforce.ibmcloud.com/vulnerabilities/216207

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.2**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mermaid - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Mermaid vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Nástroj je používaný aj v Gitlabe.

Dátum prvého zverejnenia varovania

29.12.2021

CVE

CVE-2021-43861

Zasiahnuté systémy

Mermaid Mermaid vo verzii staršej ako 8.13.8

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://github.com/mermaid-js/mermaid/security/advisories/GHSA-p3rp-vmj9-gv6v
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43861
https://exchange.xforce.ibmcloud.com/vulnerabilities/216437

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SuiteCRM - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja SuiteCRM vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

28.12.2021

CVE

CVE-2021-45903

Zasiahnuté systémy

SuiteCRM vo verzii staršej ako 8.0.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://github.com/ach-ing/cves/blob/main/CVE-2021-45903.md
https://suitecrm.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45903
https://exchange.xforce.ibmcloud.com/vulnerabilities/216191

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bitmask Riseup VPN produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bitmask vydala bezpečnostnú aktualizáciu na produkt Riseup VPN, ktorá opravuje bezpečnostnú zraniteľnosť.
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.

Dátum prvého zverejnenia varovania

30.12.2021

CVE

CVE-2021-44466

Zasiahnuté systémy

Bitmask Riseup VPN vo verzii staršej ako 0.21.11

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.tenable.com/security/research/tra-2021-58
https://bitmask.net/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44466
https://exchange.xforce.ibmcloud.com/vulnerabilities/216440