BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 09. 2020 - 06. 10. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	NVIDIA ovládače - viacero zraniteľností	Vysoká	**8.8**
02.	SevOne Network Management System	Vysoká	**8.8**
03.	Trend Micro Antivirus for MAC - zraniteľnosť	Vysoká	**7.8**
04.	Cisco Small Business RV340 Series - viacero zraniteľností	Vysoká	**7.3**
05.	Škodlivý kód v moduloch Node.js	Vysoká	**7.1**

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-236

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

Identifikátor

NVIDIA ovládače - viacero zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie svojich ovládačov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by lokálny autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

30.09.2020

CVE

CVE-2020-5979, CVE-2020-5980, CVE-2020-5981, CVE-2020-5982, CVE-2020-5983, CVE-2020-5984, CVE-2020-5985, CVE-2020-5986, CVE-2020-5987, CVE-2020-5988, CVE-2020-5989

Zasiahnuté systémy

NVIDIA® GPU Display Driver verzie upresnené v bulletine spoločnosti NVIDIA

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu NVIDIA ovládačov.
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://nvidia.custhelp.com/app/answers/detail/a_id/5075

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

Identifikátor

SevOne Network Management System

Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých zraniteľnostiach v produkte SevOne Network Management System.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených CSV súborov alebo odosielaním špeciálne vytvorených HTTP požiadaviek mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.10.2020

CVE

-

Zasiahnuté systémy

SevOne Network Management System (NMS) verzie 5.7.2.22

Následky

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

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní 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://seclists.org/fulldisclosure/2020/Oct/5

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

Identifikátor

Trend Micro Antivirus for MAC - zraniteľnosť

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na produktrend Micro Antivirus for Mac, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v implementačnej chybe v module iTISPlugin a lokálny autentifikovaný útočník by ju mohol zneužíť na eskaláciu privilégií a výkonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

01.10.2020

CVE

CVE-2020-25776

Zasiahnuté systémy

Trend Micro Antivirus for Mac verzie 9.0.1379

Následky

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

Odporúčania

Administrátorom a pouťívateľom 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://exchange.xforce.ibmcloud.com/vulnerabilities/189190
https://www.zerodayinitiative.com/advisories/ZDI-20-1236/
https://helpcenter.trendmicro.com/en-us/article/TMKA-09924

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

Identifikátor

Cisco Small Business RV340 Series - viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na routre Cisco Small Business RV340 Series, ktoré opravujú dve bezpečnostné zraniteľnosti.
Zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.09.2020

CVE

CVE-2020-3451, CVE-2020-3453

Zasiahnuté systémy

Cisco Small Business Routers s firmwarom verzie 1.0.03.19 a staršie

Následky

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

Odporúčania

Administrátorom 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-osinj-rce-pwTkPCJv

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

Identifikátor

Škodlivý kód v moduloch Node.js

Popis

Bezpečnostní výskumníci informovali o prítomnosti škodlivého kódu v Node.js moduloch electorn a loadyaml. Uvedené pluginy po inštalácii spustili predinštalovaný skript, ktorý exfiltroval citivé údaje (IP adresa, geolokácia, domovský priečinok aplikácie, používateľké meno) na verejný Github repozitár vo forme verejných komentárov.
Uvedené moduly boli odstránené z NPM registra a exfiltrovaný obsah bol ostránený z Github.

Dátum prvého zverejnenia varovania

01.10.2020

CVE

-

Zasiahnuté systémy

Node.js electorn
Node.js loadyaml

Následky

Vykonanie škodlivého kódu a exfiltrácia dát
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú predmetné Node.js moduly. V prípade, že áno, administrátorom odporúčame bezodkladné odstránenie pluginov.
Rovnako odporúčame vykonať kontrolu systému a zmenu všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch.

Zdroje

https://www.npmjs.com/advisories/1563
https://www.npmjs.com/advisories/1562
https://exchange.xforce.ibmcloud.com/vulnerabilities/189191
https://exchange.xforce.ibmcloud.com/vulnerabilities/189192