BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 03. 2019 - 02. 04. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	PHOENIX CONTACT FL NAT SMN 8TX zraniteľnosť	Vysoká	**8.8**
02.	NVIDIA GeForce Experience zraniteľnosť	Vysoká	**8.8**
03.	CMS Made Simple viacero zraniteľností	Vysoká	**8.8**
04.	Cisco IOS viacero zraniteľností	Vysoká	**8.8**
05.	Nagios XI zraniteľnosť	Vysoká	**8.8**
06.	Apache mod_auth_mellon viacero zraniteľností	Vysoká	**8.6**
07.	ENTTEC Lighting Controllers zraniteľnosť	Vysoká	**7.5**
08.	ABUS Secvest Remote Control viacero zraniteľností	Vysoká	**7.5**
09.	Nouveau Display Driver zraniteľnosť	Vysoká	**7.4**

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:
01380/2019/TS/OKB-096

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

Identifikátor

PHOENIX CONTACT FL NAT SMN 8TX zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v sieťových zariadeniach PHOENIX CONTACT FL NAT SMN 8TX.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov vo WEB-UI a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

25.03.2019

CVE

CVE-2019-9744

Zasiahnuté systémy

PHOENIX CONTACT FL NAT SMN 8TX-M (2702443)
PHOENIX CONTACT FL NAT SMN 8TX-M-DMG (2989352)
PHOENIX CONTACT FL NAT SMN 8TX (2989365)
PHOENIX CONTACT FL NAT SMCS 8TX (2989378)

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vypnúť WEB-UI a na administráciu používať prístup prostredníctvom SNMP.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2019-006

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

Identifikátor

NVIDIA GeForce Experience zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v ich produkte NVIDIA GeForce Experience.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.03.2019

CVE

CVE-2019-5674

Zasiahnuté systémy

NVIDIA GeForce Experience verzie staršie ako 3.18.0.94

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bleepingcomputer.com/news/security/nvidia-patches-high-severity-geforce-experience-vulnerability/
https://news.softpedia.com/news/security-flaw-discovered-in-nvidia-geforce-experience-update-recommended-asap-525460.shtml

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

Identifikátor

CMS Made Simple viacero zraniteľností

Popis

Bezpečnostní výskumníci objavili viacero zraniteľností v systéme pre správu obsahu CMS Made Simple. Najzávažnejšie zraniteľnosti sú spôsobená nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.03.2019

CVE

CVE-2019-10105, CVE-2019-10106, CVE-2019-10107, CVE-2019-9053, CVE-2019-9055, CVE-2019-9057, CVE-2019-9058, CVE-2019-9059, CVE-2019-9061

Zasiahnuté systémy

CMS Made Simple verzia 2.2.8
CMS Made Simple verzia 2.2.10

Následky

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

Odporúčania

Na zraniteľnosť aktuálne neexistuje bezpečnostná záplata.
Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://nvd.nist.gov/vuln/detail/CVE-2019-9053
https://nvd.nist.gov/vuln/detail/CVE-2019-9055
https://nvd.nist.gov/vuln/detail/CVE-2019-9057
https://nvd.nist.gov/vuln/detail/CVE-2019-9058
https://nvd.nist.gov/vuln/detail/CVE-2019-9059
https://nvd.nist.gov/vuln/detail/CVE-2019-9061
https://nvd.nist.gov/vuln/detail/CVE-2019-10105
https://nvd.nist.gov/vuln/detail/CVE-2019-10106
https://nvd.nist.gov/vuln/detail/CVE-2019-10107

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

Identifikátor

Cisco IOS viacero zraniteľností

Popis

Spoločnosť Cisco vydala aktualizácie na svoje produkty Cisco IOS a Cisco IOS XE ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.03.2019

CVE

CVE-2019-1737, CVE-2019-1738, CVE-2019-1739, CVE-2019-1740, CVE-2019-1741, CVE-2019-1742, CVE-2019-1743, CVE-2019-1745, CVE-2019-1746, CVE-2019-1747, CVE-2019-1748, CVE-2019-1749, CVE-2019-1750, CVE-2019-1751, CVE-2019-1752, CVE-2019-1753, CVE-2019-1754, CVE-2019-1755, CVE-2019-1756

Zasiahnuté systémy

Cisco IOS
Cisco IOS XE

Následky

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

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/viewErp.x?alertId=ERP-71135
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-xecmd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-iosxe-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-iosxe-pe

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

Identifikátor

Nagios XI zraniteľnosť

Popis

Spoločnosť Nagios vydala aktualizáciu na svoj produkt ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.03.2019

CVE

CVE-2019-9164

Zasiahnuté systémy

Nagios XI verzie staršie ako 5.5.11

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://www.nagios.com/downloads/nagios-xi/change-log/
https://nvd.nist.gov/vuln/detail/CVE-2019-9164

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache mod_auth_mellon viacero zraniteľností

Popis

Bezpečnostní výskumníci objavili viacero zraniteľností v Apache mod_auth_mellon module. Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

22.03.2019

CVE

CVE-2019-3877, CVE-2019-3878

Zasiahnuté systémy

Apache mod_auth_mellon 0.14.1

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/Uninett/mod_auth_mellon/commit/e09a28a30e13e5c22b481010f26b4a7743a09280
https://github.com/Uninett/mod_auth_mellon/commit/62041428a32de402e0be6ba45fe12df6a83bedb8
https://exchange.xforce.ibmcloud.com/vulnerabilities/158550
https://exchange.xforce.ibmcloud.com/vulnerabilities/158551

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

Identifikátor

ENTTEC Lighting Controllers zraniteľnosť

Popis

Spoločnosť ENTTEC vydala bezpečnostné aktualizácie na svoje produkty Datagate MK2, Storm 24 a Pixelator, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi reštartovať zariadenie a tým spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

26.03.2019

CVE

CVE-2019-6542

Zasiahnuté systémy

ENTTEC Datagate MK2 verzie staršie ako 70044_update_05032019-482
ENTTEC Storm 24 verzie staršie ako 70050_update_05032019-482
ENTTEC Pixelator verzie staršie ako 70060_update_05032019-482

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-085-03-0

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

Identifikátor

ABUS Secvest Remote Control viacero zraniteľností

Popis

Bezpečnostní výskumníci objavili viacero zraniteľností v diaľkových ovládačoch na elektronické zabezpečovacie systémy Abus Secvest.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.03.2019

CVE

CVE-2019-9860, CVE-2019-9862, CVE-2019-9863

Zasiahnuté systémy

ABUS Secvest Remote Control (FUBE50014, FUBE50015)
ABUS Secvest (FUAA50000) v3.01.01

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Na zraniteľnosť aktuálne neexistuje bezpečnostná záplata.
Používateľom zasiahnutých zabezpečovacích systémov odporúčame pri ich obsluhe nepoužívať diaľkové ovládania a aplikovať elektromagnetické zatienenie rádiového prijímača riadiacej jednotky.

Zdroje

https://seclists.org/bugtraq/2019/Mar/37
https://seclists.org/bugtraq/2019/Mar/38
https://exchange.xforce.ibmcloud.com/vulnerabilities/158552
https://exchange.xforce.ibmcloud.com/vulnerabilities/158553
https://exchange.xforce.ibmcloud.com/vulnerabilities/158554

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

Identifikátor

Nouveau Display Driver zraniteľnosť

Popis

Vývojári Nouveau Display Driver vydali aktualizáciu na svoj produkt ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.03.2019

CVE

CVE-2018-3979

Zasiahnuté systémy

Nouveau Display Driver NV117 (vermagic: 4.15.0-29-generic SMP mod_unload)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0647