BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 12. 2020 - 22. 12. 2020

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-293

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

Identifikátor

Viacero zraniteľností v Apple produktoch

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť nachádzajúca sa v produkte macOS Big Sur je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi, prostredíctvom podvrhnutia špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby alebo vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.12.2020

CVE

CVE-2020-10002, CVE-2020-10004, CVE-2020-10006, CVE-2020-10007, CVE-2020-10008, CVE-2020-10009, CVE-2020-10010, CVE-2020-10012, CVE-2020-10014, CVE-2020-10015, CVE-2020-10016, CVE-2020-10017, CVE-2020-13524, CVE-2020-15969, CVE-2020-27896, CVE-2020-27897, CVE-2020-27898, CVE-2020-27899, CVE-2020-27900, CVE-2020-27901, CVE-2020-27903, CVE-2020-27906, CVE-2020-27907, CVE-2020-27908, CVE-2020-27910, CVE-2020-27911, CVE-2020-27912, CVE-2020-27914, CVE-2020-27915, CVE-2020-27916, CVE-2020-27919, CVE-2020-27920, CVE-2020-27921, CVE-2020-27922, CVE-2020-27923, CVE-2020-27924, CVE-2020-27926, CVE-2020-27931, CVE-2020-27941, CVE-2020-27943, CVE-2020-27944, CVE-2020-27946, CVE-2020-27947, CVE-2020-27948, CVE-2020-27949, CVE-2020-27951, CVE-2020-27952, CVE-2020-29611, CVE-2020-29612, CVE-2020-29613, CVE-2020-29616, CVE-2020-29617, CVE-2020-29618, CVE-2020-29619, CVE-2020-29620, CVE-2020-29621, CVE-2020-9849, CVE-2020-9942, CVE-2020-9943, CVE-2020-9944, CVE-2020-9955, CVE-2020-9956, CVE-2020-9960, CVE-2020-9962, CVE-2020-9963, CVE-2020-9967, CVE-2020-9971, CVE-2020-9974, CVE-2020-9975, CVE-2020-9977, CVE-2020-9978, CVE-2020-9991, CVE-2020-9995

Zasiahnuté systémy

Apple watchOS verzie staršie ako 7.2 and 6.3
Apple macOS verzie staršie ako Big Sur 11.1,
Apple macOS verzie staršie ako Security Update 2020-001 Catalina
Apple macOS verzie staršie ako Security Update 2020-007 Mojave
Apple tvOS verzie staršie ako tvOS 14.3
Apple iOS verzie staršie ako 14.3 and 12.5
Apple iPadOS verzie staršie ako 14.3
Apple macOS Server verzie staršie ako 5.11
Apple Safari verzie staršie ako 14.0.2

Následky

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky. 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://support.apple.com/sk-sk/HT212003 https://support.apple.com/sk-sk/HT212004 https://support.apple.com/sk-sk/HT212005 https://support.apple.com/sk-sk/HT212006 https://support.apple.com/sk-sk/HT212007 https://support.apple.com/sk-sk/HT212009 https://support.apple.com/sk-sk/HT212011 https://support.apple.com/sk-sk/HT211932 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2020-167/ https://nvd.nist.gov/vuln/detail/CVE-2020-27906

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

Identifikátor

Zraniteľnosti v produktoch Mozilla

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svojho e-mailového klienta Thunderbird a prehliadač Firefox, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného e-mailu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.12.2020

CVE

CVE-2020-16042, CVE-2020-26971, CVE-2020-26972, CVE-2020-26973, CVE-2020-26974, CVE-2020-26975, CVE-2020-26976, CVE-2020-26977, CVE-2020-26978, CVE-2020-26979, CVE-2020-35111, CVE-2020-35112, CVE-2020-35113, CVE-2020-35114

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 78.6
Mozilla Firefox verzie staršie ako 84
Mozilla Firefox ESR verzie staršie ako 78.6

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 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 bolo používané rovnaké heslo alebo kľúč.

Zdroje

https://access.redhat.com/security/cve/cve-2020-16042
https://www.mozilla.org/en-US/security/advisories/mfsa2020-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-56/

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

Identifikátor

Zraniteľnosti v SolarWinds N-Central

Popis

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie na svoj produkt N-Central, ktorí opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s používateľskými právami vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.12.2020

CVE

CVE-2020-25617, CVE-2020-25618, CVE-2020-25619, CVE-2020-25620, CVE-2020-25621, CVE-2020-25622

Zasiahnuté systémy

SolarWinds N-Central vo verzii staršej ako 2020.1 HF2

Následky

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

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 bolo používané rovnaké heslo alebo kľúč.

Zdroje

https://insinuator.net/2020/12/security-advisories-for-solarwinds-n-central/
https://documentation.solarwindsmsp.com/N-central/Rel_2020-1-2_HF2/N-central_2020-1-2_HF2_ReleaseNotes_en.pdf
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25618
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25621
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25622

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

Identifikátor

Bezpečnostná zraniteľnosť v Emerson Rosemount X-STREAM Gas Analyzer

Popis

Spoločnosť Emerson vydala bezpečnostné aktualizácie pre svoj produkt Rosemount X-STREAM Gas Analyzer, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.12.2020

CVE

CVE-2020-27254

Zasiahnuté systémy

X-STREAM enhanced XEGP všetky verzie
X-STREAM enhanced XEGK všetky verzie
X-STREAM enhanced XEFD všetky verzie
X-STREAM enhanced XEXF všetky verzie

Následky

Neoprávnený prístup k citlivým údajom

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

Zdroje

https://www.emerson.com/documents/automation/xstream-notification-add-vulner-r1-en-7238500.pdf
https://us-cert.cisa.gov/ics/advisories/icsa-20-352-01

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

Identifikátor

Zraniteľnosti vo WAGO 750-88x a 750-352

Popis

Spoločnosť WAGO vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.11.2020

CVE

CVE-2020-12516

Zasiahnuté systémy

WAGO 750-352 verzie staršie ako FW14
WAGO 750-831/xxx-xxx verzie staršie ako FW14
WAGO 750-852 verzie staršie ako FW14
WAGO 750-880/xxx-xxx verzie staršie ako FW14
WAGO 750-881 verzie staršie ako FW14
WAGO 750-889 verzie staršie ako FW14
WAGO 750-331/xxx-xxx verzie staršie ako FW14
WAGO 750-829 verzie staršie ako FW14
WAGO 750-882 verzie staršie ako FW14
WAGO 750-885 verzie staršie ako FW14

Následky

Zneprístupnenie služby

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-308-01