BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 11. 2020 - 17. 11. 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-268

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 produkty macOS Big Sur, High Sierra, Mojave a Safari, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.11.2020

CVE

CVE-2019-14899, CVE-2019-20838, CVE-2020-10002, CVE-2020-10003, CVE-2020-10004, CVE-2020-10006, CVE-2020-10007, CVE-2020-10009, CVE-2020-10010, CVE-2020-10012, CVE-2020-10014, CVE-2020-10016, CVE-2020-10017, CVE-2020-10663, CVE-2020-13434, CVE-2020-13435, CVE-2020-13524, CVE-2020-13630, CVE-2020-13631, CVE-2020-14155, CVE-2020-15358, CVE-2020-27894, CVE-2020-27896, CVE-2020-27898, CVE-2020-27900, CVE-2020-27903, CVE-2020-27904, CVE-2020-27906, CVE-2020-27910, CVE-2020-27911, CVE-2020-27912, CVE-2020-27916, CVE-2020-27917, CVE-2020-27918, CVE-2020-27927, CVE-2020-27930, CVE-2020-27932, CVE-2020-27950, CVE-2020-9849, CVE-2020-9876, CVE-2020-9883, CVE-2020-9941, CVE-2020-9942, CVE-2020-9943, CVE-2020-9944, CVE-2020-9945, CVE-2020-9949, CVE-2020-9963, CVE-2020-9965, CVE-2020-9966, CVE-2020-9969, CVE-2020-9974, CVE-2020-9977, CVE-2020-9988, CVE-2020-9989, CVE-2020-9991, CVE-2020-9996, CVE-2020-9999

Zasiahnuté systémy

Safari verzie staršie ako 14.0.1
macOS Big Sur verzie staršie ako 11.0.1
macOS High Sierra verzie staršie ako 10.13.6
macOS Mojave verzie staršie ako 10.14.6

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a súbory z neznámych zdrojov.
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.

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-268

Zdroje
https://support.apple.com/sk-sk/HT201222 https://support.apple.com/sk-sk/HT211946 https://support.apple.com/sk-sk/HT211934 https://support.apple.com/sk-sk/HT211931

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

Identifikátor

Bezpečnostné zraniteľnosti v produktoch Mozzila Thunderbird a Firefox

Popis

Spoločnosť Firefox vydala bezpečnostné aktualizácie na svoje produkty Thunderbird a Firefox, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód.
Niektoré zo zraniteľností sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

17.11.2020

CVE

CVE-2020-15999, CVE-2020-16012, CVE-2020-26951, CVE-2020-26952, CVE-2020-26953, CVE-2020-26954, CVE-2020-26955, CVE-2020-26956, CVE-2020-26957, CVE-2020-26958, CVE-2020-26959, CVE-2020-26960, CVE-2020-26961, CVE-2020-26962, CVE-2020-26963, CVE-2020-26964, CVE-2020-26965, CVE-2020-26966, CVE-2020-26967, CVE-2020-26968, CVE-2020-26969

Zasiahnuté systémy

Firefox verzie staršie ako 83
Firefox ESR verzie staršie ako 78.5
Thunderbird verzie staršie ako 78.5

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a súbory z neznámych zdrojov.
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.mozilla.org/en-US/security/advisories/mfsa2020-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-50/

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

Identifikátor

Viacero bezpečnostných zraniteľností GitLab

Popis

Spoločnosť GitLab vydala bezpečnostnú aktualizáciu na svoj produkt GitLab, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej požiadavky získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.11.2020

CVE

CVE-2020-13348, CVE-2020-13349, CVE-2020-13350, CVE-2020-13351, CVE-2020-13352, CVE-2020-13353, CVE-2020-13354, CVE-2020-13355, CVE-2020-13356, CVE-2020-13358, CVE-2020-13359, CVE-2020-13360, CVE-2020-26405, CVE-2020-26406

Zasiahnuté systémy

GitLab CE/EE všetky verzie od 8.8.9. do 13.3.9

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, ktoré mohli spôsobiť únik citlivých údajov, 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://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13356.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13355.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13348.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13349.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13350.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13351.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13352.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13353.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13354.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13358.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13359.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13360.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26405.json
https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26406.json

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-268

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Firefox VPN zraniteľnosť

Popis

Spoločnosť Firefox vydala bezpečnostné aktualizácie na svoje VPN produkty pre platformy Android, iOS a Windows, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL adresy získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.11.2020

CVE

CVE-2020-15679

Zasiahnuté systémy

Mozilla VPN Android verzie staršie ako 1.1.0 (1360)
Mozilla VPN iOS verzie staršie ako 1.0.7 (929)
Mozilla VPN Windows verzie staršie ako 1.2.2

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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 zraniteľnosti, ktoré mohli spôsobiť únik citlivých informácií, 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.mozilla.org/en-US/security/advisories/mfsa2020-48/#CVE-2020-15679

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostné zraniteľnosti ProcessMaker

Popis

Bezpečnostní výskumníci zverejnili informácie o dvoch bezpečnostných zraniteľnostiach automatizačnej platformy ProcessMaker.
Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému autenfikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

17.11.2020

CVE

CVE-2020-13525, CVE-2020-13526

Zasiahnuté systémy

ProcessMaker všetky verzie staršie ako 3.4.11 (vrátane)

Následky

Vykonanie škodlivého kódu

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL)
Po odstránení zraniteľnosti, 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://talosintelligence.com/vulnerability_reports/TALOS-2020-1126