BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 10. 2022 - 02. 11. 2022

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:
01794/2022/SK-CERT-926

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.2**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v kerneli operačných systémov iOS a iPadOS, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právami používateľa prostredníctvom podvrhnutia špeciálne vytvorenej aplikácie eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

24.10.2022

CVE

CVE-2021-36690, CVE-2021-39537, CVE-2022-0261, CVE-2022-0318, CVE-2022-0319, CVE-2022-0351, CVE-2022-0359, CVE-2022-0361, CVE-2022-0368, CVE-2022-0392, CVE-2022-0554, CVE-2022-0572, CVE-2022-0629, CVE-2022-0685, CVE-2022-0696, CVE-2022-0714, CVE-2022-0729, CVE-2022-0943, CVE-2022-1381, CVE-2022-1420, CVE-2022-1616, CVE-2022-1619, CVE-2022-1620, CVE-2022-1621, CVE-2022-1622, CVE-2022-1629, CVE-2022-1674, CVE-2022-1720, CVE-2022-1725, CVE-2022-1733, CVE-2022-1735, CVE-2022-1769, CVE-2022-1851, CVE-2022-1897, CVE-2022-1898, CVE-2022-1927, CVE-2022-1942, CVE-2022-1968, CVE-2022-2000, CVE-2022-2042, CVE-2022-2124, CVE-2022-2125, CVE-2022-2126, CVE-2022-26730, CVE-2022-28739, CVE-2022-29458, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-32827, CVE-2022-32858, CVE-2022-32862, CVE-2022-32864, CVE-2022-32865, CVE-2022-32866, CVE-2022-32867, CVE-2022-32870, CVE-2022-32875, CVE-2022-32879, CVE-2022-32881, CVE-2022-32883, CVE-2022-32886, CVE-2022-32888, CVE-2022-32890, CVE-2022-32892, CVE-2022-32895, CVE-2022-32898, CVE-2022-32899, CVE-2022-32902, CVE-2022-32904, CVE-2022-32905, CVE-2022-32908, CVE-2022-32911, CVE-2022-32912, CVE-2022-32913, CVE-2022-32914, CVE-2022-32915, CVE-2022-32918, CVE-2022-32922, CVE-2022-32924, CVE-2022-32928, CVE-2022-32934, CVE-2022-32936, CVE-2022-32938, CVE-2022-32940, CVE-2022-32946, CVE-2022-32947, CVE-2022-3437, CVE-2022-42788, CVE-2022-42789, CVE-2022-42790, CVE-2022-42791, CVE-2022-42793, CVE-2022-42795, CVE-2022-42796, CVE-2022-42799, CVE-2022-42806, CVE-2022-42808, CVE-2022-42809, CVE-2022-42811, CVE-2022-42813, CVE-2022-42814, CVE-2022-42815, CVE-2022-42818, CVE-2022-42819, CVE-2022-42820, CVE-2022-42823, CVE-2022-42824, CVE-2022-42825, CVE-2022-42827, CVE-2022-42829, CVE-2022-42830, CVE-2022-42831, CVE-2022-42832

Zasiahnuté systémy

Apple Safari vo verzii staršej ako 16.1
Apple iOS 16.1 a iPadOS vo verzii staršej ako 16
macOS Big Sur vo verzii staršej ako 11.7.1
Apple Apple macOS Monterey vo verzii staršej ako 12.6.1
Apple macOS Ventura vo verzii staršej ako 13
Apple tvOS vo verzii staršej ako 16.1
Apple watchOS vo verzii staršej ako 9.1

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať bezodkladnú 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 vykonanie škodlivého kódu 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://support.apple.com/en-us/HT201222 https://support.apple.com/en-us/HT213488 https://support.apple.com/en-us/HT213489 https://support.apple.com/en-us/HT213491 https://support.apple.com/en-us/HT213492 https://support.apple.com/en-us/HT213493 https://support.apple.com/en-us/HT213494 https://support.apple.com/en-us/HT213495 https://www.cybersecurity-help.cz/vdb/SB2022102435 https://isc.sans.edu/forums/diary/Apple+Patches+Everything+October+2022+Edition/29182

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

Identifikátor

Cisco AnyConnect Secure Mobility Client pre Windows - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt AnyConnect Secure Mobility Client pre Windows, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemumu, autentifikovanému útočníkovi s právami používateľa prostredníctvom zaslania špeciálne vytvorenej IPC (interprocess communication) správy vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

25.10.2022

CVE

CVE-2020-3153, CVE-2020-3433

Zasiahnuté systémy

Cisco AnyConnect Secure Mobility Client pre Windows vo verzii staršej ako 4.9.00086

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj

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

Identifikátor

SQLite - bezpečnostná zraniteľnosť

Popis

Vývojári databázového nástroja SQLite vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.10.2022

CVE

CVE-2022-35737

Zasiahnuté systémy

SQLite vo verzii staršej ako 3.39.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2022-35737
https://thehackernews.com/2022/10/22-year-old-vulnerability-reported-in.html

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

Identifikátor

OpenSSL knižnica - dve bezpečnosté zraniteľnosti

Popis

Vývojári knižnice OpenSSL vydali bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného X.509 certifikátu spôsobiť zneprístupnenie služby a v obmedzených prípadoch vykonať škodlivý kód.
K uvedenej zraniteľnosti je v súčasnosti dostupný proof of concept (POC) kód

Dátum prvého zverejnenia varovania

28.10.2022

CVE

CVE-2022-3602, CVE-2022-3786

IOC

OpenSSL vo verzii staršej ako 3.0.7
OpenSSL vo verziách 1.1.1 a 1.0.2 nie sú zasiahnuté

Zasiahnuté systémy

Následky

Zneprístupnenie služby
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov.
Taktiež odporúčame nepovolovať načítavanie nedôverihodných certifikátov.
Identifikácia zraniteľných knižníc môže byť vykonaná prostredníctvom YARA pravidla zverejnenom na webovej adrese https://www.sk-cert.sk/sk/kriticka-zranitelnost-v-openssl-potreba-zabezpecit-systemovych-administratorov-na-utorok-1-11-2022-sviatok-vsetkych-svatych/index.html

Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu 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://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/ https://github.com/NCSC-NL/OpenSSL-vulnerability-2022 https://isc.sans.edu/forums/diary/Upcoming+Critical+OpenSSL+Vulnerability+What+will+be+Affected/29192/ https://www.sk-cert.sk/sk/kriticka-zranitelnost-v-openssl-potreba-zabezpecit-systemovych-administratorov-na-utorok-1-11-2022-sviatok-vsetkych-svatych/index.html