NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÉ VAROVANIE

No: V20200528-01K

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti Apple produktov

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností. Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.05.2020

CVE

CVE-2019-14868, CVE-2019-20044, CVE-2019-20503, CVE-2020-3878, CVE-2020-3882, CVE-2020-6616, CVE-2020-9771, CVE-2020-9772, CVE-2020-9788, CVE-2020-9789, CVE-2020-9790, CVE-2020-9791, CVE-2020-9792, CVE-2020-9793, CVE-2020-9794, CVE-2020-9795, CVE-2020-9797, CVE-2020-9800, CVE-2020-9801, CVE-2020-9802, CVE-2020-9803, CVE-2020-9804, CVE-2020-9805, CVE-2020-9806, CVE-2020-9807, CVE-2020-9808, CVE-2020-9809, CVE-2020-9811, CVE-2020-9812, CVE-2020-9813, CVE-2020-9814, CVE-2020-9815, CVE-2020-9816, CVE-2020-9817, CVE-2020-9818, CVE-2020-9819, CVE-2020-9820, CVE-2020-9821, CVE-2020-9822, CVE-2020-9823, CVE-2020-9824, CVE-2020-9825, CVE-2020-9826, CVE-2020-9827, CVE-2020-9828, CVE-2020-9829, CVE-2020-9830, CVE-2020-9831, CVE-2020-9832, CVE-2020-9833, CVE-2020-9834, CVE-2020-9835, CVE-2020-9837, CVE-2020-9838, CVE-2020-9839, CVE-2020-9841, CVE-2020-9842, CVE-2020-9843, CVE-2020-9844, CVE-2020-9847, CVE-2020-9848, CVE-2020-9850, CVE-2020-3878, CVE-2020-9851, CVE-2020-9852, CVE-2020-9855, CVE-2020-9856, CVE-2020-9857, CVE-2020-9858,

IOC

-

Zasiahnuté systémy

macOS Catalina verzie staršie ako 10.15.5, Security Update 2020-003 Mojave a Security Update 2020-003 High Sierra
Windows Migration Assistant verzie staršie ako 2.2.0.0
iOS verzie staršie ako 13.5
iPadOS verzie staršie ako 13.5
Safari verzie staršie ako 13.1.1
iCloud for Windows verzie staršie ako 11.2 a 7.19

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-128

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

Odporúčania
Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie. 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/en-us/HT211179 https://support.apple.com/en-us/HT211168 https://support.apple.com/en-us/HT211186 https://support.apple.com/en-us/HT211181 https://support.apple.com/en-us/HT211170 https://support.apple.com/en-us/HT211177 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2020-071/ https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2020-072/ https://www.bleepingcomputer.com/news/security/german-govt-urges-ios-users-to-patch-critical-mail-app-flaws/ https://www.securityweek.com/apple-patches-over-40-vulnerabilities-macos-catalina

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-128