BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 05. 2020 - 02. 06. 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-131

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

Identifikátor

Johnson Controls Kantech EntraPass zraniteľnosť

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt Kantech EntraPass, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

26.05.2020

CVE

CVE-2020-9046

Zasiahnuté systémy

Johnson Controls Kantech EntraPass verzie staršie ako 8.23

Následky

Eskalácia privilégií

Odporúčania

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

Zdroje

https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2020/jci-psa-2020-6-v1-kantech-entrapass-security-management-software.pdf?la=en&hash=2CC411E20B2BC12B9CE733BA6628740FD925DBA5
https://www.us-cert.gov/ics/advisories/icsa-20-147-02

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

Identifikátor

Apple iOS zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie svoje produkty, ktoré opravujú zero day bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.06.2020

CVE

CVE-2020-9859

Zasiahnuté systémy

Apple iOS verzie staršie ako 13.5.1
Apple iPadOS verzie staršie ako 13.5.1
Apple tvOS verzie staršie ako 13.4.6
Apple macOS Catalina verzie staršie ako 10.15.5 Supplemental Update a Security Update 2020-003 High Sierra
Apple watchOS verzie staršie ako 6.2.6

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/HT211214
https://support.apple.com/en-us/HT211216
https://support.apple.com/en-us/HT211217
https://support.apple.com/en-us/HT211215
https://duo.com/decipher/ios-13-5-1-fixes-kernel-zero-day
https://news.ycombinator.com/item?id=23381675
https://exchange.xforce.ibmcloud.com/vulnerabilities/182741

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

Identifikátor

Cisco produkty zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na portfólio svojich produktov používajúcich Cisco NX-OS, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v sieťovom rozhraní Cisco NX-OS je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

01.06.2020

CVE

CVE-2020-10136

Zasiahnuté systémy

Nexus 1000 Virtual Edge for VMware vSphere
Nexus 1000V Switch for Microsoft Hyper-V
Nexus 1000V Switch for VMware vSphere
Nexus 3000 Series Switches
Nexus 5500 Platform Switches
Nexus 5600 Platform Switches
Nexus 6000 Series Switches
Nexus 7000 Series Switches
Nexus 9000 Series Switches in standalone NX-OS mode
Cisco UCS 6200 a 6300 verzie staršie ako 3.2(3o), 4.0(4i) a 4.1(1d)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipip-dos-kCT9X4

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

Identifikátor

FreeRDP viacero zraniteľností

Popis

Vývojári FreeRDP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

29.05.2020

CVE

CVE-2020-11017, CVE-2020-11018, CVE-2020-11019, CVE-2020-11038, CVE-2020-11039, CVE-2020-11040, CVE-2020-11041, CVE-2020-11043, CVE-2020-11085, CVE-2020-11086, CVE-2020-11087, CVE-2020-11088, CVE-2020-11089

Zasiahnuté systémy

FreeRDP verzie staršie ako 2.1.0

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Používateľom Microsoft MSTSC odporúčame vypnúť funkciu obojstranného zdieľania obsahu schránky prostredníctvom RDP.

Zdroje

https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-wvrr-2f4r-hjvh
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-w67c-26c4-2h9w
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-fg8v-w34r-c974
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-84vj-g73m-chw7
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-hfc7-c5gv-8c2h
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-xh4f-fh87-43hp
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-h25x-cqr6-fp6g
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-2j4w-v45m-95hf
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mx9p-f6q8-mqwq
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-x4wq-m7c9-rjgr
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-5mr4-28w3-rc84
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-q5c8-fm29-q57c
https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8cvc-vcw7-6mfw
https://nvd.nist.gov/vuln/detail/CVE-2020-11017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware produkty viacero zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty ESXi, VMRC, Workstation, Fusion a Horizon, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente TOCTOU a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

28.05.2020

CVE

CVE-2020-3957, CVE-2020-3958, CVE-2020-3959

Zasiahnuté systémy

VMware Workstation verzie staršie ako 15.5.2
VMware Fusion verzie staršie ako 11.5.5
VMware ESXi verzie staršie ako 7.0, 6.7 ESXi670-202004101-SG a 6.5 ESXi650-202005401-SG
VMRC for Mac
Horizon Client for Mac

Následky

Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2020-0011.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell Dock Firmware Update Utilities zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty Dock Firmware Update Utilities, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

30.05.2020

CVE

CVE-2020-5357

Zasiahnuté systémy

Dell Dock WD15 verzie staršie ako 1.0.8
Dell Dock WD19 verzie staršie ako 1.0.14
Dell Thunderbolt Dock TB16 verzie staršie ako 1.0.4
Thunderbolt Dock - TB18DC verzie staršie ako 1.0.10

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.dell.com/support/article/sk-sk/SLN321564
https://nvd.nist.gov/vuln/detail/CVE-2020-5357