BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 09. 2020 - 29. 09. 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-230

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

Identifikátor

Microsoft Edge - viacero zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Edge, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

Dátum prvého zverejnenia varovania

23.09.2020

CVE

CVE-2020-15960, CVE-2020-15961, CVE-2020-15962, CVE-2020-15963, CVE-2020-15964, CVE-2020-15965, CVE-2020-15966

Zasiahnuté systémy

MS Edge verzie staršie ako 85.0.564.63

Následky

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

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://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200002

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

Identifikátor

Cisco IOS a IOS EX - viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na Cisco IOS a Cisco IOS XE, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom.

Dátum prvého zverejnenia varovania

24.09.2020

CVE

CVE-2020-3141, CVE-2020-3359, CVE-2020-3390, CVE-2020-3399, CVE-2020-3400, CVE-2020-3407, CVE-2020-3408, CVE-2020-3409, CVE-2020-3414, CVE-2020-3416, CVE-2020-3417, CVE-2020-3421, CVE-2020-3422, CVE-2020-3425, CVE-2020-3426, CVE-2020-3428, CVE-2020-3429, CVE-2020-3465, CVE-2020-3480, CVE-2020-3486, CVE-2020-3487, CVE-2020-3488, CVE-2020-3489, CVE-2020-3492, CVE-2020-3493, CVE-2020-3494, CVE-2020-3497, CVE-2020-3508, CVE-2020-3509, CVE-2020-3510, CVE-2020-3511, CVE-2020-3512, CVE-2020-3513, CVE-2020-3524, CVE-2020-3526, CVE-2020-3527, CVE-2020-3552, CVE-2020-3560

Zasiahnuté systémy

Cisco IOS
Cisco IOS XE Software

Aironet 1540 Series APs
Aironet 1560 Series APs
Aironet 1800 Series APs
Aironet 2800 Series APs
Aironet 3800 Series APs
Aironet 4800 APs
Business 100 Series APs and Mesh Extenders
Business 200 Series APs
Catalyst 9100 APs
Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
Catalyst 9800 Series Wireless Controllers
Catalyst IW 6300 APs
Cisco 4461 Integrated Services Routers
ESW6300 Series APs
Embedded Wireless Controller on Catalyst 9100 Access Points
Integrated Access Point on 1100 Integrated Services Routers

Následky

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

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.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironet-dos-VHr2zG9y
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewlc-snmp-dos-wNkedg9K
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capwap-dos-ShFzXf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-auth-bypass-6j2BYUc7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confacl-HbPtfSuO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esp20-arp-dos-GvHVggqJ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-rsp3-rce-jVHg8Z7c
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-le-drTOB625
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-ethport-dos-xtjTt8pY
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-COPS-VLD-MpbTvGEW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rommon-secboot-7JgVLVYC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-profinet-dos-65qYG3W5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-isdn-q931-dos-67eUZBTf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-splitdns-SPWqpdGW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xbace-OnCEbyS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wpa-dos-cXshjerc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-JP-DOS-g5FfGm8y
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-umbrella-dos-t2QMUX37
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-dhcp-dos-JSCKX43h
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dclass-dos-VKh9D8k3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mdns-dos-3tH6cA9J
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-priv-esc-K8zvEWM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-profinet-J9QMCHPB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-wlc-fnfv9-EvrAQpNX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISR4461-gKKUROhx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-lpwa-access-cXsD7PRA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-zbfw-94ckG4G
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsla-jw2DJmSv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capwap-dos-TPdNTdyq

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

Identifikátor

Apple macOS a iCloud - viacero zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie, ktoré opravujú viacero chýb a bezpečnostných zraniteľností v operačnom systéme macOS a aplikácii iCloud pre Windows.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.09.2020

CVE

CVE-2020-9941, CVE-2020-9952, CVE-2020-9961, CVE-2020-9968, CVE-2020-9973

Zasiahnuté systémy

macOS Catalina staršie ako 10.15.7
iCloud pre Windows verzie staršie ako 11.4

Následky

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

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.

Zdroje

https://support.apple.com/en-us/HT211849
https://support.apple.com/en-us/HT211846

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

Identifikátor

Trend Micro Apex One, OfficeScan, Security 2020 - viacero zraniteľností

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoje produkty Apex One, OfficeScan a Security 2020, ktoré opravujú viaceré zraniteľnosti.
Najzávažnejšie zraniteľnosti by lokálny neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.09.2020

CVE

CVE-2020-24562, CVE-2020-24563, CVE-2020-24564, CVE-2020-24565, CVE-2020-25770, CVE-2020-25771, CVE-2020-25772, CVE-2020-25773, CVE-2020-25774, CVE-2020-25775

Zasiahnuté systémy

Trend Micro Apex One verzie pred Sept 2020 Monthly Patch
Trend Micro OfficeScan verzie pred XG SP1 Patch 3 b5684
Trend Micro Security verzie pred 2020 (v16) ActiveUpdate a 2021 (v17)

Následky

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

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.

Zdroje

https://success.trendmicro.com/solution/000271974
https://success.trendmicro.com/solution/000263633
https://helpcenter.trendmicro.com/en-us/article/TMKA-09909

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

Identifikátor

Foxit Reader a PhantomPDF - viacero zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoje produkty Reader a PhantomPDF, ktorá opravuje viacero zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.09.2020

CVE

CVE-2020-17410, CVE-2020-17411, CVE-2020-17413, CVE-2020-17414, CVE-2020-17415, CVE-2020-17416, CVE-2020-17417

Zasiahnuté systémy

Foxit Reader verzie 10.0.1.35811 a staršie
Foxit PhantomPDF verzie 10.0.1.35811 a staršie

Následky

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

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 sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PrestaShop - viacero zraniteľností

Popis

Vývojári e-commerce platformy PrestaShop vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ich mohol zneužiť na vykonanie XSS útoku a získanie prístupu k údajom uloženým v cookies.
Zraniteľnosť s označením CVE-2020-15160 by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v databáze.

Dátum prvého zverejnenia varovania

24.09.2020

CVE

CVE-2020-15160, CVE-2020-15161, CVE-2020-15162

Zasiahnuté systémy

PrestaShop verzie staršie ako 1.7.6.8

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na platforme PrestaShop v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Po vykonaní aktualizácie odporúčame preveriť integritu databázy (napr. vytvorené používateľské účty) a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/189139
https://exchange.xforce.ibmcloud.com/vulnerabilities/189140
https://exchange.xforce.ibmcloud.com/vulnerabilities/189142

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

Identifikátor

QEMU - viacero zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o kritických bezpečnostných zraniteľnostiach v produkte QEMU.
Zraniteľnosti by lokálny neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.09.2020

CVE

CVE-2020-25741, CVE-2020-25742, CVE-2020-25743

Zasiahnuté systémy

QEMU

Následky

Zneprístupnenie služby

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2020/q3/201
https://lists.nongnu.org/archive/html/qemu-devel/2020-09/msg07779.html