BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 07. 2021 - 27. 07. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Cisco Intersight Virtual Appliance - dve bezpečnostné zraniteľnosti	Vysoká	**8.3**
02.	Fortinet FortiManager a FortiAnalyzer - bezpečnostná zraniteľnosť	Vysoká	**8.1**
03.	MB connect line produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
04.	Drupal core - bezpečnostná zraniteľnosť	Vysoká	**7.8**
05.	Mitsubishi Electric MELSEC-F séria produktov - bezpečnostná zraniteľnosť	Vysoká	**7.5**
06.	Citrix ADC, Gateway a SD-WAN WANOP produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.5**

Dôležitosť	**☐ Nízka**	**☐ Stredná**	**☒ Vysoká**	**☐ Kritická**	**CVSS skóre: 8.3**
Klasifikácia	**☒ Neutajované / TLP(CLEAR)**		**☐ Vyhradené**	**☐ Dôverné**	**☐ Tajné**
Kód sektora (dopad)					

Identifikátor
Cisco Intersight Virtual Appliance - dve bezpečnostné zraniteľnosti

Popis
Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Intersight Virtual Appliance, ktorá opravuje bezpečnostnú zraniteľnosť. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne upravených paketov, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania
21.07.2021

CVE
CVE-2021-1600, CVE-2021-1601

Zasiahnuté systémy
Cisco Intersight Virtual Appliance vo verzii staršej ako 1.0.9-292

Následky
Neoprávnený prístup k citlivým údajom Neoprávnená zmena v systéme Zneprístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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-ucsi2-iptaclbp-L8Dzs8m8

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

Identifikátor
Fortinet FortiManager a FortiAnalyzer - bezpečnostná zraniteľnosť

Popis
Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu na produkty FortiManager a FortiAnalyzer, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom znovupoužitia uvoľnenej pamäte, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania
19.07.2021

CVE
CVE-2021-32589

Zasiahnuté systémy
FortiManager vo verzii staršej ako 5.6.11 FortiManager vo verzii staršej ako 6.0.11 FortiManager vo verzii staršej ako 6.2.8 FortiManager vo verzii staršej ako 6.4.6 FortiManager vo verzii staršej ako 7.0.1 FortiAnalyzer vo verzii staršej ako 5.6.11 FortiAnalyzer vo verzii staršej ako 6.0.11 FortiAnalyzer vo verzii staršej ako 6.2.8 FortiAnalyzer vo verzii staršej ako 6.4.6 FortiAnalyzer vo verzii staršej ako 7.0.1

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

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.fortiguard.com/psirt/FG-IR-21-067 https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/fortinet-releases-security-updates-fortimanager-and-fortianalyzer

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

Identifikátor

MB connect line produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť MB connect line vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.07.2021

CVE

CVE-2020-9497, CVE-2020-9498, CVE-2021-33526, CVE-2021-33527, CVE-2021-34574, CVE-2021-34575

Zasiahnuté systémy

mbDIALUP vo verzii staršej ako 3.9R0.5
mbCONNECT24 vo verzii staršej ako 2.9.0
mymbCONNECT24 vo verzii staršej ako 2.9.0

Následky

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

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://cert.vde.com/en-us/advisories/vde-2021-030
https://cert.vde.com/en-us/advisories/vde-2021-031
https://cert.vde.com/en-us/advisories/vde-2021-017

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

Identifikátor

Drupal core - bezpečnostná zraniteľnosť

Popis

Vývojári CMS Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.07.2021

CVE

CVE-2021-32610

Zasiahnuté systémy

Drupal vo verzii staršej ako 9.2.2

Drupal vo verzii staršej ako 9.1.11

Drupal vo verzii staršej ako 8.9.17

Drupal vo verzii staršej ako 7.82

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

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.drupal.org/sa-core-2021-004

https://exchange.xforce.ibmcloud.com/vulnerabilities/206016

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

Identifikátor
Mitsubishi Electric MELSEC-F séria produktov - bezpečnostná zraniteľnosť

Popis
Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na produkty série MELSEC-F, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených paketov, spôsobiť znepřístupnenie služby.

Dátum prvého zverejnenia varovania
26.07.2021

CVE
CVE-2021-20596

Zasiahnuté systémy
FX3U-ENET s firmware vo verzii staršej ako 1.16 FX3U-ENET-L s firmware vo verzii staršej ako 1.16 FX3U-ENET-P502 s firmware vo verzii staršej ako 1.16

Následky
Znepřístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://us-cert.cisa.gov/ics/advisories/icsa-21-201-01

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

Identifikátor

Citrix ADC, Gateway a SD-WAN WANOP produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Citrix vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

19.07.2021

CVE

CVE-2021-22919, CVE-2021-22920, CVE-2021-22927

Zasiahnuté systémy

Citrix ADC a Citrix Gateway vo verzii staršej ako 13.0-82.45
Citrix ADC a Citrix Gateway vo verzii staršej ako 12.1-62.27
Citrix ADC a NetScaler Gateway vo verzii staršej ako 11.1-65.22
Citrix ADC 12.1-FIPS vo verzii staršej ako 12.1-55.247
Citrix SD-WAN WANOP Edition vo verzii staršej ako 11.4.0a
Citrix SD-WAN WANOP Edition vo verzii staršej ako 11.3.2a
Citrix SD-WAN WANOP Edition vo verzii staršej ako 11.2.3b
Citrix SD-WAN WANOP Edition vo verzii staršej ako 10.2.9b

Následky

Znepristupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.citrix.com/article/CTX319135
https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/citrix-releases-security-updates
https://exchange.xforce.ibmcloud.com/vulnerabilities/205706
https://exchange.xforce.ibmcloud.com/vulnerabilities/205705
https://exchange.xforce.ibmcloud.com/vulnerabilities/205707