BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 06. 2021 - 06. 07. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	AVEVA System Platform - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
02.	Dell BIOSConnect a HTTPS Boot - viacero bezpečnostných zraniteľností	Vysoká	**8.3**
03.	NVIDIA GeForce Experience - bezpečnostná zraniteľnosť	Vysoká	**8.3**
04.	Western Digital My Book Live a Live Duo - bezpečnostná zraniteľnosť	Vysoká	**7.5**
05.	Fortinet FortiWeb - bezpečnostná zraniteľnosť	Vysoká	**7.4**
06.	PHOENIX CONTACT produkty - dve bezpečnostné zraniteľnosti	Vysoká	**7.4**

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-467

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

Identifikátor

AVEVA System Platform - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť AVEVA Software vydala bezpečnostnú aktualizáciu na produkt System Platform, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.06.2021

CVE

CVE-2021-33008, CVE-2021-33010

Zasiahnuté systémy

System Platform 2020 R2 P01 vo verzii staršej ako AVEVA Communication Drivers Pack 2020 R2.1
System Platform 2020 2020 R2 vo verzii staršej ako AVEVA Communication Drivers Pack 2020 R2.1
System Platform 2020 2020 vo verzii staršej ako AVEVA Communication Drivers Pack 2020 R2.1
System Platform 2017 U3 SP1 P01 vo verzii staršej ako AVEVA Communication Drivers Pack 2020 R2.1

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-180-05

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

Identifikátor

Dell BIOSConnect a HTTPS Boot - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty BIOSConnect a HTTPS Boot, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom pretečenia zásobníka, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.06.2021

CVE

CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574

Zasiahnuté systémy

BIOSConnect
HTTPS Boot
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://www.dell.com/support/kbdoc/sk-sk/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-bioscconnect-feature-and-https-boot-feature

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

Zdroje

https://www.dell.com/support/kbdoc/sk-sk/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-bioscconnect-feature-and-https-boot-feature
https://gizmodo.com/30-million-dell-devices-have-preinstalled-software-with-1847168297
https://thehackernews.com/2021/06/bios-disconnect-new-high-severity-flaws.html
https://www.cybersafe.news/dell-bioscconnect-code-execution-bugs-affect-millions-of-devices/

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

Identifikátor

NVIDIA GeForce Experience - bezpečnostná zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostnú aktualizáciu na svoj produkt GeForce Experience, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej URL, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.06.2021

CVE

-

Zasiahnuté systémy

GeForce Experience pre Windows vo verzii staršej ako 3.23

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

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5199
https://threatpost.com/nvidia-high-severity-geforce-spoof-bug/167345/

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

Identifikátor

Western Digital My Book Live a Live Duo - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Western Digital My Book Live Duo.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov, spôsobiť zneprístupnenie služby.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

29.06.2021

CVE

CVE-2021-35941

Zasiahnuté systémy

My Book Live WDBACG0030HCH
My Book Live WDBACG0020HCH
My Book Live WDBACG0010HCH
My Book Live Duo WDBVHT0080JCH
My Book Live Duo WDBVHT0060JCH
My Book Live Duo WDBVHT0040JCH

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom a používateľom odporúčame prevádzkovať My Book Live a Live Duo úplne oddelené od internetu.

Zdroje

https://www.westerndigital.com/support/productsecurity/wdc-21008-recommended-security-measures-wd-mybooklive-wd-mybookliveduo
https://threatpost.com/zero-day-wipe-my-book-live/167422/
https://arstechnica.com/gadgets/2021/06/hackers-exploited-0-day-not-2018-bug-to-mass-wipe-my-book-live-devices/
https://vuldb.com/?id.177755
https://www.securityweek.com/zero-day-vulnerability-exploited-recent-attacks-wd-storage-devices
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35941

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Fortinet FortiWeb - bezpečnostná zraniteľnosť

Popis

Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu na svoj produkt FortiWeb, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.06.2021

CVE

CVE-2021-22123

Zasiahnuté systémy

FortiWeb vo verzii staršej ako 6.3.8
FortiWeb vo verzii staršej ako 6.2.4

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://www.securityweek.com/vulnerabilities-expose-fortinet-firewalls-remote-attacks
https://www.fortiguard.com/psirt/FG-IR-20-120

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PHOENIX CONTACT produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť PHOENIX CONTACT vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

23.06.2021

CVE

CVE-2021-3449, CVE-2021-3450

Zasiahnuté systémy

AXC F 1152 s firmware vo verzii staršej ako 2021.0.5 LTS
AXC F 2152 s firmware vo verzii staršej ako 2021.0.5 LTS
AXC F 3152 s firmware vo verzii staršej ako 2021.0.5 LTS
RFC 4072S s firmware vo verzii staršej ako 2021.0.5 LTS
AXC F 2152 Starterkit s firmware vo verzii staršej ako 2021.0.5 LTS
PLCnext Technology Starterkit s firmware vo verzii staršej ako 2021.0.5 LTS
FL MGUARD DM UNLIMITED s firmware vo verzii staršej ako 1.13
TC ROUTER 3002T-4G s firmware vo verzii staršej ako 2.06.5
TC ROUTER 2002T-3G s firmware vo verzii staršej ako 2.06.5
TC ROUTER 3002T-4G s firmware vo verzii staršej ako 2.06.5
TC ROUTER 2002T-3G s firmware vo verzii staršej ako 2.06.5
TC ROUTER 3002T-4G VZW s firmware vo verzii staršej ako 2.06.5
TC ROUTER 3002T-4G ATT s firmware vo verzii staršej ako 2.06.5
CLOUD CLIENT 1101T-TX/TX s firmware vo verzii staršej ako 2.06.5
TC ROUTER 4002T-4G EU s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
TC ROUTER 4102T-4G EU WLAN s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
TC ROUTER 4202T-4G EU WLAN s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
CLOUD CLIENT 2002T-4G EU s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
CLOUD CLIENT 2002T-WLAN s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
CLOUD CLIENT 2102T-4G EU WLAN s firmware vo verzii staršej ako 4.5.72.100 (vrátane)
ILC 2050 BI s firmware vo verzii staršej ako 1.5.1
ILC 2050 BI-L s firmware vo verzii staršej ako 1.5.1
SMARTRTU AXC SG s firmware vo verzii staršej ako V1.6.0.1
SMARTRTU AXC IG s firmware vo verzii staršej ako V1.0.0.0
ENERGY AXC PU s firmware vo verzii staršej ako V4.10.0.0

Následky
Neoprávnený prístup k citlivým údajom Neoprávnená zmena v systéme

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. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://cert.vde.com/en-us/advisories/vde-2021-025