BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 09. 2020 - 15. 09. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe produkty - viacero zraniteľností	Vysoká	**8.8**
02.	Google Chrome - viacero zraniteľností	Vysoká	**8.8**
03.	Google Android - viacero zraniteľností	Vysoká	**8.8**
04.	Fuji Electric Tellus Lite V-Simulator 6 - viacero zraniteľností	Vysoká	**8.8**
05.	Nitro Pro 13 - viacero zraniteľností	Vysoká	**8.8**
06.	Siemens produkty - zraniteľnosti	Vysoká	**8.4**
07.	McAfee Agent - viacero zraniteľností	Vysoká	**8.2**
08.	IBM Spectrum Protect Plus - viacero zraniteľností	Vysoká	**8.0**
09.	Schneider Electric SCADAPack - viacero zraniteľností	Vysoká	**7.8**
10.	FATEK Automation PLC WinProladder - zraniteľnosť	Vysoká	**7.8**
11.	WordPress Email Subscribers & Newsletters plugin - zraniteľnosť	Vysoká	**7.5**
12.	Adobe Media Encoder - viacero zraniteľností	Vysoká	**7.5**
13.	F5 BIG-IP - bezpečnostná zraniteľnosť	Vysoká	**7.4**
14.	Philips zdravotnícke monitorovacie zariadenia - viacero zraniteľností	Stredná	**6.8**
15.	VMware produkty - viacero zraniteľností	Stredná	**6.7**

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-223

BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 09. 2020 - 15. 09. 2020

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

Identifikátor

Adobe produkty - viacero zraniteľností

Popis

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

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2020-9725, CVE-2020-9726, CVE-2020-9727, CVE-2020-9728, CVE-2020-9729, CVE-2020-9730, CVE-2020-9731, CVE-2020-9732, CVE-2020-9733, CVE-2020-9734, CVE-2020-9735, CVE-2020-9736, CVE-2020-9737, CVE-2020-9738, CVE-2020-9740, CVE-2020-9741, CVE-2020-9742, CVE-2020-9743

Zasiahnuté systémy

Adobe Experience Manager (AEM) verzie staršie ako 6.5.6.0 a 6.4.8.2
AEM Forms add-on verzie staršie ako AEM Forms Service Pack 6
Adobe Framemaker verzie staršie ako 2019.0.7
Adobe InDesign verzie staršie ako 15.1.2

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://helpx.adobe.com/security/products/experience-manager/apsb20-56.html
https://helpx.adobe.com/security/products/framemaker/apsb20-54.html
https://helpx.adobe.com/security/products/indesign/apsb20-52.html
https://www.scmagazine.com/home/patch-management/adobe-patches-for-critical-flaws-should-be-applied-right-away/
https://www.theregister.com/2020/09/08/patch_tuesday_september/
https://exchange.xforce.ibmcloud.com/vulnerabilities/187866
https://exchange.xforce.ibmcloud.com/vulnerabilities/187867
https://exchange.xforce.ibmcloud.com/vulnerabilities/187864
https://exchange.xforce.ibmcloud.com/vulnerabilities/187863

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

Identifikátor

Google Chrome - viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2020-15959, CVE-2020-6573, CVE-2020-6574, CVE-2020-6575, CVE-2020-6576

Zasiahnuté systémy

Google Chrome verzie staršie ako 85.0.4183.102

Následky

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

Odporúčania

Administrátorom 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://chromereleases.googleblog.com/2020/09/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/187893
https://exchange.xforce.ibmcloud.com/vulnerabilities/187895
https://exchange.xforce.ibmcloud.com/vulnerabilities/187896

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

Identifikátor

Google Android - viacero zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj operačný systém Android, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2019-10527, CVE-2019-10596, CVE-2019-10628, CVE-2019-10629, CVE-2019-13992, CVE-2019-13994, CVE-2019-13995, CVE-2019-14074, CVE-2019-14117, CVE-2020-0074, CVE-2020-0123, CVE-2020-0229, CVE-2020-0245, CVE-2020-0278, CVE-2020-0342, CVE-2020-0379, CVE-2020-0380, CVE-2020-0381, CVE-2020-0382, CVE-2020-0383, CVE-2020-0384, CVE-2020-0385, CVE-2020-0386, CVE-2020-0388, CVE-2020-0389, CVE-2020-0390, CVE-2020-0391, CVE-2020-0392, CVE-2020-0393, CVE-2020-0394, CVE-2020-0395, CVE-2020-0396, CVE-2020-0397, CVE-2020-0399, CVE-2020-0401, CVE-2020-0402, CVE-2020-0404, CVE-2020-0407, CVE-2020-11124, CVE-2020-11129, CVE-2020-11133, CVE-2020-11135, CVE-2020-3613, CVE-2020-3617, CVE-2020-3620, CVE-2020-3621, CVE-2020-3622, CVE-2020-3629, CVE-2020-3634, CVE-2020-3656, CVE-2020-3671

Zasiahnuté systémy

Operačný systém Android so Security Patch Levels staršími ako 2020-09-05

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://source.android.com/security/bulletin/2020-09-01

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

Identifikátor

Fuji Electric Tellus Lite V-Simulator 6 - viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o viacerých zraniteľnostiach v produkte Fuji Electric Tellus Lite V-Simulator 6.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2020-10646

Zasiahnuté systémy

Fuji Electric Tellus Lite V-Simulator 6

Následky

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

Odporúčania

Bezpečnostné aktualizácie riešiace uvedené zraniteľnosti doposiaľ neboli vydané.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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.zerodayinitiative.com/advisories/ZDI-20-1117/
https://www.zerodayinitiative.com/advisories/ZDI-20-1116/
https://www.zerodayinitiative.com/advisories/ZDI-20-1115/
https://www.zerodayinitiative.com/advisories/ZDI-20-1114/
https://www.zerodayinitiative.com/advisories/ZDI-20-1113/
https://www.zerodayinitiative.com/advisories/ZDI-20-1112/
https://www.zerodayinitiative.com/advisories/ZDI-20-1111/
https://www.zerodayinitiative.com/advisories/ZDI-20-1110/
https://www.zerodayinitiative.com/advisories/ZDI-20-1109/
https://www.zerodayinitiative.com/advisories/ZDI-20-1108/
https://www.zerodayinitiative.com/advisories/ZDI-20-1107/
https://www.zerodayinitiative.com/advisories/ZDI-20-1106/
https://www.zerodayinitiative.com/advisories/ZDI-20-1105/
https://www.zerodayinitiative.com/advisories/ZDI-20-1104/
https://www.zerodayinitiative.com/advisories/ZDI-20-1103/

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

Identifikátor

Nitro Pro 13 - viacero zraniteľností

Popis

Spoločnosť Nitro vydala bezpečnostnú aktualizáciu na svoj produkt Nitro Pro 13, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.09.2020

CVE

CVE-2020-6112, CVE-2020-6113, CVE-2020-6115, CVE-2020-6116, CVE-2020-6146

Zasiahnuté systémy

Nitro Pro 13 verzie staršie ako 13.24.1.467

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://www.gonitro.com/nps/security/updates
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1063
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1084
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1070
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1068
https://talosintelligence.com/vulnerability_reports/TALOS-2020-1062

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty - zraniteľnosti

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2020-0543, CVE-2020-10049, CVE-2020-10050, CVE-2020-10051, CVE-2020-10056, CVE-2020-15784, CVE-2020-15785, CVE-2020-15786, CVE-2020-15787, CVE-2020-15788, CVE-2020-15789, CVE-2020-15790, CVE-2020-15791

Zasiahnuté systémy

SIMATIC RTLS Locating Manager verzie staršie ako 2.10.2
SIMATIC S7-300 CPU
SIMATIC S7-400 CPU
SIMATIC HMI Basic Panels
SIMATIC HMI Comfort Panels
SIMATIC HMI Mobile Panels
SIMATIC HMI United Comfort Panels
SIMATIC Field PG M4
SIMATIC Field PG M5
SIMATIC Field PG M6
SIMATIC IPC3000 SMART
SIMATIC IPC347E
SIMATIC IPC427D
SIMATIC IPC427E
SIMATIC IPC477D
SIMATIC IPC477E
SIMATIC IPC477E Pro
SIMATIC IPC527G
SIMATIC IPC547E
SIMATIC IPC547G
SIMATIC IPC627D
SIMATIC IPC627E
SIMATIC IPC647D
SIMATIC IPC647E
SIMATIC IPC677D
SIMATIC IPC677E
SIMATIC IPC827D
SIMATIC IPC847D
SIMATIC IPC847E
SIMATIC ITP1000
SIMOTION P320-4E
SIMOTION P320-4S
SINUMERIK 828D (PPU.4 / PPU1740)
SINUMERIK 840D sl (NCU730.3B)
SINUMERIK ONE (NCU1750 / NCU1760)
Polarion Subversion Webclient
License Management Utility (LMU) verzie staršie ako 2.4
Spectrum Power verzie staršie ako 4.70 SP8
Siveillance Video Client

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

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

Zdroje
https://cert-portal.siemens.com/productcert/txt/ssa-251935.txt
https://cert-portal.siemens.com/productcert/txt/ssa-381684.txt
https://cert-portal.siemens.com/productcert/txt/ssa-436520.txt
https://cert-portal.siemens.com/productcert/txt/ssa-534763.txt
https://cert-portal.siemens.com/productcert/txt/ssa-542525.txt
https://cert-portal.siemens.com/productcert/txt/ssa-568969.txt
https://cert-portal.siemens.com/productcert/txt/ssa-709003.txt
https://cert-portal.siemens.com/productcert/txt/ssa-770698.txt
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-08
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-06
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-05
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-04
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-03
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

McAfee Agent - viacero zraniteľností

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt McAfee Agent, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

09.09.2020

CVE

CVE-2020-7311, CVE-2020-7312, CVE-2020-7314, CVE-2020-7315

Zasiahnuté systémy

McAfee Agent verzie staršie ako 5.6.6

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kc.mcafee.com/corporate/index?page=content&id=SB10325
https://exchange.xforce.ibmcloud.com/vulnerabilities/188090
https://exchange.xforce.ibmcloud.com/vulnerabilities/188091

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Spectrum Protect Plus - viacero zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Spectrum Protect Plus, ktorá opravuje bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.09.2020

CVE

CVE-2020-4703, CVE-2020-4711

Zasiahnuté systémy

IBM Spectrum Protect Plus verzie staršie ako 10.1.5.2199

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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.ibm.com/support/pages/node/6328867
https://www.tenable.com/security/research/tra-2020-54
https://exchange.xforce.ibmcloud.com/vulnerabilities/187188

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

Identifikátor

Schneider Electric SCADAPack - viacero zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje produkty SCADAPack, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených .sdb súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.09.2020

CVE

CVE-2020-7528, CVE-2020-7529, CVE-2020-7530, CVE-2020-7531, CVE-2020-7532

Zasiahnuté systémy

Schneider Electric SCADAPack 7x RemoteConnect verzie staršie ako V3.7.3.904
Schneider Electric SCADAPack x70 Security Administrator verzie staršie ako V1.6.2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-252-01_SCADAPack_RemoteConnect_and_Security_Administrator.pdf

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

Identifikátor

FATEK Automation PLC WinProladder - zraniteľnosť

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte FATEK Automation PLC WinProladder.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených .spf a .tab súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2020

CVE

CVE-2020-16234

Zasiahnuté systémy

FATEK Automation PLC WinProladder verzia 3.28 a staršie

Následky

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

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedenú zraniteľnosť doposiaľ nebola vydaná.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/188238
https://exchange.xforce.ibmcloud.com/vulnerabilities/188237
https://www.zerodayinitiative.com/advisories/ZDI-20-1173/
https://www.zerodayinitiative.com/advisories/ZDI-20-1174/
https://us-cert.cisa.gov/ics/advisories/icsa-20-254-02

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

Identifikátor

WordPress Email Subscribers & Newsletters plugin - zraniteľnosť

Popis

Vývojári WordPress zásuvného modulu Email Subscribers & Newsletters vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a rozposielať podvrhnuté e-mailové správy.

Dátum prvého zverejnenia varovania

09.09.2020

CVE

CVE-2020-5780

Zasiahnuté systémy

WordPress Email Subscribers & Newsletters plugin verzie staršie ako 4.5.6

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress so zraniteľnou verziou pluginu. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginu.
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://threatpost.com/wordpress-plugin-flaw/159172/
https://www.tenable.com/security/research/tra-2020-53
https://nvd.nist.gov/vuln/detail/CVE-2020-5780

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

Identifikátor

Adobe Media Encoder - viacero zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu svojho produktu Media Encoder, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.09.2020

CVE

CVE-2020-9739, CVE-2020-9744, CVE-2020-9745

Zasiahnuté systémy

Adobe Media Encoder verzie staršie ako 14.4

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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.

Zdroje

https://helpx.adobe.com/security/products/media-encoder/apsb20-57.html

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

Identifikátor

F5 BIG-IP - bezpečnostná zraniteľnosť

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.09.2020

CVE

CVE-2020-5929

Zasiahnuté systémy

BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO) verzie staršie ako 14.0.0, 13.1.0, 13.0.0 HF3, 12.1.3, 12.1.2 HF2, 11.6.3, 11.6.2 HF1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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.

Zdroje

https://support.f5.com/csp/article/K91158923
https://exchange.xforce.ibmcloud.com/vulnerabilities/188064

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Philips zdravotnícke monitorovacie zariadenia - viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o viacerých zraniteľnostiach v zdravotníckych monitorovacích zariadeniach výrobcu Philips.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k citlivým údajom a tiež spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.09.2020

CVE

CVE-2020-16212, CVE-2020-16214, CVE-2020-16216, CVE-2020-16218, CVE-2020-16220, CVE-2020-16222, CVE-2020-16224, CVE-2020-16228

Zasiahnuté systémy

Philips Patient Information Center iX (PICiX) verzie B.02, C.02, C.03
Philips PerformanceBridge Focal Point verzia A.01
Philips IntelliVue patient monitors MX100, MX400-MX850, MP2-MP90
Philips IntelliVue X3 a X2

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Bezpečnostné aktualizácie riešiace uvedené zraniteľnosti doposiaľ neboli vydané.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-20-254-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware produkty - viacero zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty Horizon, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Fusion umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

14.09.2020

CVE

CVE-2020-3980, CVE-2020-3986, CVE-2020-3987, CVE-2020-3988, CVE-2020-3989, CVE-2020-3990

Zasiahnuté systémy

VMware Horizon Client for Windows verzie staršie ako 5.4.4
VMware Workstation 15.x
VMware Fusion 11.x

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://www.zerodayinitiative.com/advisories/ZDI-20-1181/
https://www.zerodayinitiative.com/advisories/ZDI-20-1180/
https://www.zerodayinitiative.com/advisories/ZDI-20-1179/
https://www.zerodayinitiative.com/advisories/ZDI-20-1178/
https://www.zerodayinitiative.com/advisories/ZDI-20-1177/

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-223