BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 05. 2020 - 19. 05. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WordPress Page Builder viacero zraniteľností	Vysoká	**8.8**
02.	Eaton Intelligent Power Manager zraniteľnosti	Vysoká	**8.8**
03.	F5 BIG-IP viacero zraniteľností	Vysoká	**8.8**
04.	TYPO3 viacero zraniteľností	Vysoká	**8.8**
05.	Dahua IP kamery a NVR zraniteľnosti	Vysoká	**8.8**
06.	Schneider Electric produkty viacero zraniteľností	Vysoká	**8.6**
07.	OSIsoft PI System zraniteľnosti	Vysoká	**7.8**
08.	PHP viacero zraniteľností	Vysoká	**7.5**

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-119

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

Identifikátor

WordPress Page Builder viacero zraniteľností

Popis

Vývojári WordPress zásuvného modulu Page Builder vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom CSRF útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.05.2020

CVE

-

Zasiahnuté systémy

Page Builder by SiteOrigin verzie staršie ako 2.10.16

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://www.wordfence.com/blog/2020/05/vulnerabilities-patched-in-page-builder-by-siteorigin-affects-over-1-million-sites/
https://www.securityweek.com/vulnerabilities-page-builder-plugin-expose-1-million-wordpress-websites

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

Identifikátor

Eaton Intelligent Power Manager zraniteľnosti

Popis

Spoločnosť Eaton vydala bezpečnostnú aktualizáciu na svoj produkt Intelligent Power Manager, ktorá opravuje bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.05.2020

CVE

CVE-2020-6651, CVE-2020-6652

Zasiahnuté systémy

Eaton Intelligent Power Manager verzie staršie ako 1.68

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

Zdroje

https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/security-bulletins/eaton-vulnerability-advisory-intelligent-power-manager-v1-1.pdf
https://www.us-cert.gov/ics/advisories/icsa-20-133-01
https://www.zerodayinitiative.com/advisories/ZDI-20-650/
https://www.zerodayinitiative.com/advisories/ZDI-20-649/

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

Identifikátor

F5 BIG-IP viacero zraniteľností

Popis

Spoločnosť F5 informovala o bezpečnostných zraniteľnostiach vo svojich produktoch BIG-IP (APM) a APM Clients.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente Edge Client je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje 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

12.05.2020

CVE

CVE-2020-5896, CVE-2020-5897, CVE-2020-5898

Zasiahnuté systémy

BIG-IP (APM) verzie 11.6.1 až 15.1.0
BIG-IP APM Clients verzie 7.1.5 až 7.1.9

Následky

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

Odporúčania

Bezpečnostná aktualizácia riešiaca uvedené zraniteľnosti doposiaľ nebola vydaná. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://support.f5.com/csp/article/K15478554
https://support.f5.com/csp/article/K69154630
https://support.f5.com/csp/article/K20346072

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

Identifikátor

TYPO3 viacero zraniteľností

Popis

Vývojári redakčného systému TYPO3 vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.05.2020

CVE

CVE-2020-10802, CVE-2020-10803, CVE-2020-10804, CVE-2020-11063, CVE-2020-11064, CVE-2020-11065, CVE-2020-11066, CVE-2020-11067, CVE-2020-11069, CVE-2020-11070, CVE-2020-12697, CVE-2020-12698, CVE-2020-12699, CVE-2020-12700

Zasiahnuté systémy

TYPO3 verzie staršie ako 9.5.17 a 10.4.2

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 TYPO3 v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
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://typo3.org/security/advisory/typo3-core-sa-2020-004
https://typo3.org/security/advisory/typo3-core-sa-2020-005
https://typo3.org/security/advisory/typo3-core-sa-2020-006
https://typo3.org/security/advisory/typo3-ext-sa-2020-006
https://typo3.org/security/advisory/typo3-ext-sa-2020-008
https://typo3.org/security/advisory/typo3-core-sa-2020-003
https://typo3.org/security/advisory/typo3-ext-sa-2020-007
https://typo3.org/security/advisory/typo3-core-sa-2020-002
https://typo3.org/security/advisory/typo3-core-sa-2020-001
https://typo3.org/security/advisory/typo3-ext-sa-2020-005
https://typo3.org/security/advisory/typo3-ext-sa-2020-004
https://exchange.xforce.ibmcloud.com/vulnerabilities/181833
https://exchange.xforce.ibmcloud.com/vulnerabilities/181832
https://exchange.xforce.ibmcloud.com/vulnerabilities/181808
https://exchange.xforce.ibmcloud.com/vulnerabilities/181807

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

Identifikátor

Dahua IP kamery a NVR zraniteľnosti

Popis

Spoločnosť Dahua vydala bezpečnostné aktualizácie na svoje IP kamery a NVR zariadenia, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.05.2020

CVE

CVE-2019-9682, CVE-2020-9502, CVE-2020-9682

Zasiahnuté systémy

DH_IPC-Consumer-Zi-Themis_EngSpn_N_V2.400.0000000.18.R.20200426
DH_IPC-Consumer-Zi-Themis_Eng_P_V2.400.0000000.18.R.20200426
DH_IPC-HX2X3X-Rhea_MultiLang_NP_Stream2_V2.800.0000015.0.R.200430
DH_IPC-HX2X3X-Rhea_MultiLang_PN_Stream2_V2.800.0000015.0.R.200430
DH_IPC-HX5XXX-Volt_MultiLang_NP_Stream3_V2.800.0000000.12.R.200319
DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3_V2.800.0000000.12.R.200319
DH_IPC-HX8XXX-Nobel_MultiLang_NP_Stream3_V2.800.0000000.5.R.200324
DH_IPC-HX8XXX-Nobel_MultiLang_NP_V2.800.0000000.5.R.200324
DH_IPC-HX8XXX-Nobel_MultiLang_PN_V2.800.0000000.5.R.200324
DH_IPC-HX25(8)XX-Molec_MultiLang_NP_V2.800.0000000.15.R.200313
DH_IPC-HX25(8)XX-Molec_MultiLang_PN_V2.800.0000000.15.R.200313
DH_NVR4XXX-4KS2_Chn_V4.001.0000000.1.R.200319
DH_NVR4XXX-4KS2_MultiLang_V4.001.0000000.1.R.200319
DH_NVR5XXX-4KS2_Chn_V4.001.0000000.1.R.200319
DH_NVR5XXX-4KS2_MultiLang_V4.001.0000000.1.R.200319
DH_SD-Prometheus_Chn_PN_Stream3_V2.800.0000009.3.R.200331
DH_SD-Prometheus_MultiLang_NP_Stream3_V2.800.0000009.3.R.200331
DH_SD-Prometheus_MultiLang_PN_Stream3_V2.800.0000009.3.R.200331
General_IPC-Consumer-Zi-Themis_Eng_N_V2.400.0000000.18.R.20200426
General_IPC-Consumer-Zi-Themis_Eng_P_V2.400.0000000.18.R.20200426
General_IPC-HX2X3X-Rhea_Eng_NP_Stream2_V2.800.0000015.0.R.200430
General_IPC-HX2X3X-Rhea_Eng_PN_Stream2_V2.800.0000015.0.R.200430
General_IPC-HX8XXX-Nobel_MultiLang_NP_Stream3_V2.800.0000000.5.R.200324
General_IPC-HX8XXX-Nobel_MultiLang_NP_V2.800.0000000.5.R.200324
General_IPC-HX8XXX-Nobel_MultiLang_PN_Stream3_V2.800.0000000.5.R.200324
General_IPC-HX8XXX-Nobel_MultiLang_PN_V2.800.0000000.5.R.200324
General_IPC-HX25(8)XX-Molec_MultiLang_NP_V2.800.0000000.15.R.200313
General_IPC-HX25(8)XX-Molec_MultiLang_PN_V2.800.0000000.15.R.200313
General_NVR4XXX-4KS2_Chn_V4.001.0000000.1.R.200319
General_NVR4XXX-4KS2_Eng_V4.001.0000000.1.R.200319
General_NVR4XXX-4KS2_MultiLang_V4.001.0000000.1.R.200319
General_NVR5XXX-4KS2_Chn_V4.001.0000000.1.R.200319
General_NVR5XXX-4KS2_Eng_V4.001.0000000.1.R.200319
General_NVR5XXX-4KS2_MultiLang_V4.001.0000000.1.R.200319
General_SD-Prometheus_Chn_PN_Stream3_V2.800.0000009.3.R.200331
General_SD-Prometheus_MultiLang_NP_Stream3_V2.800.0000009.3.R.200331
General_SD-Prometheus_MultiLang_PN_Stream3_V2.800.0000009.3.R.200331

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.dahuasecurity.com/support/cybersecurity/details/777
https://www.dahuasecurity.com/support/cybersecurity/details/767
https://nvd.nist.gov/vuln/detail/CVE-2019-9682

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

Identifikátor

Schneider Electric produkty viacero zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Vijeo Designer spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.05.2020

CVE

CVE-2020-7492, CVE-2020-7499, CVE-2020-7500, CVE-2020-7501

Zasiahnuté systémy

Vijeo Designer Basic verzie staršie ako V1.1 HotFix 17
Schneider Electric GP-Pro EX
U.Motion verzie staršie ako 1.4.2

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-133-03_U.motion_Servers_and_Touch_Panels_Notification.pdf&p_Doc_Ref=SEVD-2020-133-03
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-133-02_Vijeo_Designer_and_Vijeo_Designer_Basic_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-133-02
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-133-01_Pro-face_GP-ProEX_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-133-01

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

Identifikátor

OSIsoft PI System zraniteľnosti

Popis

Spoločnosť OSIsoft informovala o viacerých zraniteľnostiach vo svojich produktoch PI System. Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.05.2020

CVE

CVE-2019-10768, CVE-2019-11358, CVE-2019-18244, CVE-2020-10600, CVE-2020-10602, CVE-2020-10604, CVE-2020-10606, CVE-2020-10608, CVE-2020-10610, CVE-2020-10614

Zasiahnuté systémy

Applications using PI Asset Framework (AF) Client versions prior to and including PI AF Client 2018 SP3 Patch 1, Version 2.10.7.283
Applications using PI Software Development Kit (SDK) versions prior to and including PI SDK 2018 SP1, Version 1.4.7.602
PI API for Windows Integrated Security versions prior to and including 2.0.2.5,
PI API versions prior to and including 1.6.8.26
PI Buffer Subsystem versions prior to and including 4.8.0.18
PI Connector for BACnet, versions prior to and including 1.2.0.6
PI Connector for CygNet, versions prior to and including 1.4.0.17
PI Connector for DC Systems RTscada, versions prior to and including 1.2.0.42
PI Connector for Ethernet/IP, versions prior to and including 1.1.0.10
PI Connector for HART-IP, versions prior to and including 1.3.0.1
PI Connector for Ping, versions prior to and including 1.0.0.54
PI Connector for Wonderware Historian, versions prior to and including 1.5.0.88
PI Connector Relay, versions prior to and including 2.5.19.0
PI Data Archive versions prior to and including PI Data Archive 2018 SP3, Version 3.4.430.460
PI Data Collection Manager, versions prior to and including 2.5.19.0
PI Integrator for Business Analytics versions prior to and including 2018 R2 SP1, Version 2.2.0.183
PI Interface Configuration Utility (ICU) versions prior to and including 1.5.0.7
PI to OCS versions prior to and including 1.1.36.0
PI Data Archive 2018 and 2018 SP2
PI Vision 2019 and prior
PI Manual Logger 2017 R2 Patch 1 and prior
RtReports Version 4.1 and prior

Následky

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

Odporúčania
Administrátorom odporúčame zabezpečiť systém podľa odporúčaní výrobcu zverejnených na https://customers.osisoft.com/s/knowledgearticle?knowledgeArticleUrl=000027554 https://customers.osisoft.com/s/knowledgearticle?knowledgeArticleUrl=000026046 Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://www.us-cert.gov/ics/advisories/icsa-20-133-02

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

Identifikátor

PHP viacero zraniteľností

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

14.05.2020

CVE

CVE-2019-11048, CVE-2020-7067

Zasiahnuté systémy

PHP verzie staršie ako 7.4.5
PHP verzie staršie ako 7.3.17
PHP verzie staršie ako 7.2.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.php.net/ChangeLog-7.php#PHP_7_4
https://www.php.net/ChangeLog-7.php#PHP_7_3
https://www.php.net/ChangeLog-7.php#PHP_7_2
https://nvd.nist.gov/vuln/detail/CVE-2020-7067
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-denial-of-service_2020-068/