BEZPEČNOSTNÝ BULLETIN

Týždeň 23. 05. 2018 – 29. 05. 2018

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:
02049/2018/TS/OKB-063

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

Identifikátor

Multiple Huawei Server Products Vulnerabilities

Popis

Spoločnosť Huawei vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v Huawei serveroch.

Najzávažnejšia je trojica bezpečnostných zraniteľností, ktoré spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ich mohol zneužiť prostredníctvom podvrhnutia špeciálne vytvorených JSON požiadaviek na modifikáciu prístupového hesla administrátorského účtu a eskaláciu privilégií v napadnutom systéme.

Posledná zraniteľnosť spočíva v nesprávnej implementácii mechanizmov autentifikácie v komponente iBMC (intelligent Baseboard Management Controller) a vzdialený neautentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálne vytvorených správ zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

23.05.2018

CVE

CVE-2018-7902, CVE-2018-7903, CVE-2018-7904, CVE-2018-7942

Zasiahnuté systémy

Huawei 1288H V5 verzie V100R005C00, 2288H V5 verzie V100R005C00, 2488 V5 verzie V100R005C00, CH121 V3/V5 verzie V100R001C00, CH121L V3/V5 verzie V100R001C00, CH140 V3 verzie V100R001C00, CH140L V3 verzie V100R001C00, CH220 V3 verzie V100R001C00, CH222 V3 verzie V100R001C00, CH242 V3 verzie V100R001C00, CH242 V5 verzie V100R001C00, RH1288 V3 verzie V100R003C00, RH2288 V3 verzie V100R003C00, RH2288H V3 verzie V100R003C00, XH310 V3 verzie V100R003C00, XH321 V3 verzie V100R003C00, XH321 V5 verzie V100R005C00, XH620 V3 verzie V100R003C00

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180523-01-json-en
http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180523-01-server-en

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

Identifikátor

SoMachine Basic XML External Entity Vulnerability

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt SoMachine Basic, ktorá opravuje bezpečnostnú zraniteľnosť v XML parseri.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a lokálny neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne upraveného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.05.2018

CVE

CVE-2018-7783

Zasiahnuté systémy

SoMachine Basic verzie staršie ako v1.6 SP1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-142-01-+SoMachine+Basic.pdf&p_Doc_Ref=SEVD-2018-142-01
https://www.scmagazine.com/schneider-electric-patches-xml-external-entity-vulnerability/article/768373/

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

Identifikátor

IBM Db2 Multiple Vulnerabilities

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt Db2, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti vo funkciách db2exmig a db2exfmt spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a lokálny autentifikovaný útočník by ich mohol zneužiť na eskaláciu privilégií, vykonanie škodlivého kódu a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti by lokálny útočník mohol zneužiť na eskaláciu privilégií a modifikáciu súborov zraniteľnej inštancie DB2.

Dátum prvého zverejnenia varovania

22.05.2018

CVE

CVE-2018-1449, CVE-2018-1450, CVE-2018-1451, CVE-2018-1452, CVE-2018-1459, CVE-2018-1488, CVE-2018-1515, CVE-2018-1544, CVE-2018-1565

Zasiahnuté systémy

IBM DB2 verzie staršie ako V11.1.3.3 iFix001

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22016140
http://www-01.ibm.com/support/docview.wss?uid=swg22016141
http://www-01.ibm.com/support/docview.wss?uid=swg22016142
http://www-01.ibm.com/support/docview.wss?uid=swg22016143
http://www-01.ibm.com/support/docview.wss?uid=swg22016181

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Moodle Multiple Vulnerabilities

Popis

Vývojári e-learningového systému Moodle vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Najvážnejšie bezpečnostné zraniteľnosti by vzdialený autentifikovaný útočník mohol prostredníctvom vytvorenia špeciálnych dotazníkových otázok zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.05.2018

CVE

CVE-2018-1133, CVE-2018-1134, CVE-2018-1135, CVE-2018-1136, CVE-2018-1137

Zasiahnuté systémy

Moodle verzie staršie ako 3.5, 3.4.3, 3.3.6, 3.2.9 a 3.1.12

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Váš e-learningový systém nie je založený na systéme Moodle v zraniteľných verziách. V prípade, že áno, bezodkladne vykonajte aktualizáciu na najnovšiu verziu.

Zdroje

https://moodle.org/mod/forum/discuss.php?d=371200
https://moodle.org/mod/forum/discuss.php?d=371199
https://moodle.org/mod/forum/discuss.php?d=371201
https://moodle.org/mod/forum/discuss.php?d=371204
https://moodle.org/mod/forum/discuss.php?d=371202
https://moodle.org/mod/forum/discuss.php?d=371203

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

Identifikátor

Joomla! Multiple Flaws

Popis

Vývojári systému pre správu obsahu Joomla! vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti sú spôsobené nesprávnym filtrovaním HTML kódu v používateľských vstupoch a vzdialený autentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a získať prístup k autentifikačným údajom obete uloženým v cookies.
Ostatné zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na neoprávnený prístup k citlivým údajom alebo modifikáciu pravidiel pre riadenie prístupu (ACL) systému Joomla!.

Dátum prvého zverejnenia varovania

15.03.2018

CVE

CVE-2018-11321, CVE-2018-11322, CVE-2018-11323, CVE-2018-11324, CVE-2018-11325, CVE-2018-11326, CVE-2018-11327, CVE-2018-11328, CVE-2018-6378

Zasiahnuté systémy

Joomla! verzie staršie ako 3.8.8

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na systéme pre správu obsahu Joomla! v zraniteľných verziách. V prípade, že áno, bezodkladne vykonajte aktualizáciu na najnovšiu verziu.

Zdroje

https://www.securitytracker.com/id/1040966
https://developer.joomla.org/security-centre/737-20180509-core-xss-vulnerability-in-the-media-manager.html
https://developer.joomla.org/security-centre/736-20180508-core-possible-xss-attack-in-the-redirect-method.html

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

Identifikátor

GNOME Web Denial of Service Vulnerability

Popis

Vývojári webového prehliadača GNOME Web (Epiphany) vydali bezpečnostnú aktualizáciu, ktorá rieši bezpečnostnú zraniteľnosť v komponente libephymain.so.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom Javascriptových volaní window.open na neexistujúce URI zneužiť na spôsobenie pádu aplikácie a zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

02.05.2018 (posledná aktualizácia 24.05.2018)

CVE

CVE-2018-11396

Zasiahnuté systémy

GNOME WEB (Epiphany) 3.28.2.1

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupne aktualizácie. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/143743
https://bugzilla.gnome.org/show_bug.cgi?id=795740

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

Identifikátor

BeaconMedaes TotalAlert Scroll Medical Air Systems Vulnerabilities

Popis

Spoločnosť BeaconMedaes vydala bezpečnostné aktualizácie na svoj produkt TotalAlert Scroll Medical Air Systems, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený neautentifikovaný útočník by ich mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.05.2018

CVE

CVE-2018-7515, CVE-2018-7518, CVE-2018-7526

Zasiahnuté systémy

BeaconMedaes TotalAlert Scroll Medical Air Systems

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-144-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BD Kiestra and InoqulA Systems Vulnerabilities

Popis

Spoločnosť Becton, Dickinson and Company (BD) vydala upozornenie na bezpečnostné zraniteľnosti nachádzajúce sa v produktoch Kiestra TLA, Kiestra WCA a InoqulA.
Bezpečnostné zraniteľnosti nachádzajúce sa v komponentoch ReadA, PerformA a Database Manager by autentifikovaný útočník mohol zneužiť na vykonanie SQL príkazov vedúcich k poškodeniu alebo úplnej strate údajov uložených v databáze.

Dátum prvého zverejnenia varovania

22.05.2018

CVE

CVE-2018-10593, CVE-2018-10595

Zasiahnuté systémy

BD Kiestra TLA
BD Kiestra WCA
BD InoqulA+ specimen processor

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Odporúčame aplikáciou firewallových pravidiel limitovať dostupnosť zasiahnutých systémov z Internetu a uistiť sa, že prístupové práva k spravovaniu zasiahnutých systémov sú delegované zodpovedným a vyškoleným pracovníkom. Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletin-bd-kiestra-tla-bd-kiestra-wca-bd-inoqula
https://ics-cert.us-cert.gov/advisories/ICSMA-18-142-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Micro Focus CMDB, CMS and UCMDB Vulnerability

Popis

Spoločnosť Micro Focus vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť prítomnú v produktoch Universal CMDB Foundation Software, CMS Server a CMDB Browser.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý Javascript kód v kontexte zobrazovanej stránky a získať prístup k autentifikačným údajom obete uloženým v cookies.

Dátum prvého zverejnenia varovania

23.05.2018

CVE

CVE-2018-6495

Zasiahnuté systémy

Micro Focus Universal CMDB Foundation Software verzie 10.20, 10.21, 10.22, 10.30, 10.31, 10.32, 10.33, 11.0
Micro Focus CMS Server 2018.05 verzie 4.10, 4.11, 4.12, 4.13, 4.14, 4.15.1
Micro Focus UCMDB Browser verzie 4.10, 4.11, 4.12, 4.13, 4.14, 4.15.1

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03164778
https://exchange.xforce.ibmcloud.com/vulnerabilities/143750

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Symantec Advanced Secure Gateway and ProxySG Authentication Bypass Vulnerability

Popis

Produkty Symantec Advanced Secure Gateway a Symantec ProxySG od spoločnosti Symantec obsahujú bezpečnostnú zraniteľnosť v implementácii autentifikácie na báze SAML (Security Assertion Markup Language).
Zraniteľnosť spočíva v nesprávnom spracovávaní XML uzlov obsahujúcich komentáre a vzdialený neautentifikovaný útočník by ju podvrhnutím špeciálne upravených SAML odpovedí mohol zneužiť na obídenie mechanizmov autentifikácie a získať tak neoprávnený prístup do systému.
Uvedenú zraniteľnosť nemožno zneužiť voči administrátorským účtom manažmentového rozhrania.

Dátum prvého zverejnenia varovania

23.05.2018 (posledná aktualizácia 25.05.2018)

CVE

CVE-2018-5241

Zasiahnuté systémy

Symantec Proxysg 6.5, 6.6, 6.7
Symantec Advanced Secure Gateway verzie 6.6, 6.7

Následky

Neoprávnený prístup do systému

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať ich aktualizáciu.

Zdroje

https://www.symantec.com/security-center/network-protection-security-advisories/SA167

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Wireshark Multiple Vulnerabilities

Popis

Vývojári analytického nástroja Wireshark vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo sieťovej prevádzky zneužiť na zneprístupnenie služieb na zasiahnutom systéme.
Zraniteľnosti sa nachádzajú v kompomentoch:
- EEE 1905.1a dissector (epan/dissectors/packet-ieee1905.c)
- RTCP dissector (epan/dissectors/packet-rtcp.c)
- DNS dissector (epan/dissectors/packet-dns.c)
- LTP dissector (epan/tvbuff.c)
- Q.931 dissector (epan/dissectors/packet-q931.c)
- RRC dissector (epan/proto.c)
- GSM A DTAP dissector (epan/dissectors/packet-gsm_a_dtap.c)
- IEEE 802.11 protocol dissector (epan/crypt/dot11decrypt.c)
- LDSS dissector (epan/dissectors/packet-ldss.c

Dátum prvého zverejnenia varovania

22.05.2018

CVE

CVE-2018-11354, CVE-2018-11355, CVE-2018-11356, CVE-2018-11357, CVE-2018-11358, CVE-2018-11359, CVE-2018-11360, CVE-2018-11361, CVE-2018-11362

Zasiahnuté systémy

Wireshark verzie nižšie ako 2.6.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2018-25.html
https://www.wireshark.org/security/wnpa-sec-2018-26.html
https://www.wireshark.org/security/wnpa-sec-2018-27.html

https://www.wireshark.org/security/wnpa-sec-2018-28.html
https://www.wireshark.org/security/wnpa-sec-2018-29.html
https://www.wireshark.org/security/wnpa-sec-2018-30.html
https://www.wireshark.org/security/wnpa-sec-2018-31.html
https://www.wireshark.org/security/wnpa-sec-2018-32.html
https://www.wireshark.org/security/wnpa-sec-2018-33.html