BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 07. 2020 - 21. 07. 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.	LibreHealth EHR - viacero zraniteľností	Vysoká	**8.8**
04.	Mozilla Thunderbird - viacero zraniteľností	Vysoká	**8.8**
05.	Jenkins - viacero zraniteľností	Vysoká	**8.0**
06.	Schneider Electric produkty - viacero zraniteľností	Vysoká	**7.9**
07.	SAP produkty - viacero zraniteľností	Vysoká	**7.7**
08.	Capsule Technologies SmartLinx Neuron 2 - zraniteľnosť	Vysoká	**7.6**
09.	Apache Tomcat - viacero zraniteľností	Vysoká	**7.5**
10.	Joomla! zraniteľnosti	Stredná	**6.3**

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-185

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

14.07.2020

CVE

CVE-2020-9646, CVE-2020-9649, CVE-2020-9650, CVE-2020-9667, CVE-2020-9668, CVE-2020-9669, CVE-2020-9670, CVE-2020-9671, CVE-2020-9672, CVE-2020-9673, CVE-2020-9681, CVE-2020-9682, CVE-2020-9688

Zasiahnuté systémy

Adobe Creative Cloud Desktop Application verzie staršie ako 5.2
Adobe Media Encoder verzie staršie ako 14.3
Adobe Genuine Service verzie staršie ako 7.1
Adobe ColdFusion 2016 verzie staršie ako Update 16
Adobe ColdFusion 2018 verzie staršie ako Update 10
Adobe Download Manager verzie staršie ako 2.0.0.529

Následky

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

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/creative-cloud/apsb20-33.html
https://helpx.adobe.com/security/products/media-encoder/apsb20-36.html
https://helpx.adobe.com/security/products/integrity_service/apsb20-42.html
https://helpx.adobe.com/security/products/coldfusion/apsb20-43.html
https://helpx.adobe.com/security/products/adm/apsb20-49.html
https://thehackernews.com/2020/07/adobe-security-patch-july.html

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 38 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

14.07.2020

CVE

CVE-2020-6510, CVE-2020-6511, CVE-2020-6512, CVE-2020-6513, CVE-2020-6514, CVE-2020-6515, CVE-2020-6516, CVE-2020-6517, CVE-2020-6518, CVE-2020-6519, CVE-2020-6520, CVE-2020-6521, CVE-2020-6522, CVE-2020-6523, CVE-2020-6524, CVE-2020-6525, CVE-2020-6526, CVE-2020-6527, CVE-2020-6528, CVE-2020-6529, CVE-2020-6530, CVE-2020-6531, CVE-2020-6533, CVE-2020-6534, CVE-2020-6535, CVE-2020-6536

Zasiahnuté systémy

Google Chrome verzie staršie ako 84.0.4147.89

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/2020/07/stable-channel-update-for-desktop.html

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

Identifikátor

LibreHealth EHR - viacero zraniteľností

Popis

Vývojári LibreHealth vydali aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.07.2020

CVE

-

Zasiahnuté systémy

LibreHealth 2.0.0.

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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://labs.bishopfox.com/advisories/librehealth-version-2.0.0-0
https://www.darkreading.com/vulnerabilities---threats/vulns-in-open-source-ehr-puts-patient-health-data-at-risk/d/d-id/1338362

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

Identifikátor

Mozilla Thunderbird - viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkt Thunderbird, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

16.07.2020

CVE

CVE-2020-12402, CVE-2020-12415, CVE-2020-12416, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12421, CVE-2020-12422, CVE-2020-12423, CVE-2020-12424, CVE-2020-12425, CVE-2020-12426, CVE-2020-15648

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 78

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://www.mozilla.org/en-US/security/advisories/mfsa2020-29/

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

Identifikátor

Jenkins - viacero zraniteľností

Popis

Vývojári produktu Jenkins vydali bezpečnostné aktualizácie svojho produktu a zásuvných modulov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním 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

15.07.2020

CVE

CVE-2020-2220, CVE-2020-2221, CVE-2020-2222, CVE-2020-2223, CVE-2020-2224, CVE-2020-2225, CVE-2020-2226, CVE-2020-2227, CVE-2020-2228

Zasiahnuté systémy

Jenkins Ansible Tower verzie staršie ako 0.9.2
Jenkins verzie staršie ako 2.245
Jenkins LTS verzie staršie ako 2.235.2
Deployer Framework Plugin verzie staršie ako 1.3
Gitlab Authentication Plugin verzie staršie ako 1.6
Matrix Authorization Strategy Plugin verzie staršie ako 2.6.2
Matrix Project Plugin verzie staršie ako 1.17

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://www.openwall.com/lists/oss-security/2020/07/15/5
https://www.jenkins.io/security/advisory/2020-07-15/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
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 SESU a Floating License Manager, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.07.2020

CVE

CVE-2019-8960, CVE-2019-8961, CVE-2020-7520

Zasiahnuté systémy

Schneider Electric Floating License Manager verzie staršie ako 2.5.0.0
Schneider Electric Schneider Electric Software Update (SESU) verzie staršie ako 2.5.0
EcoStruxure Augmented Operator Advisor
EcoStruxure Control Expert (Unity Pro)
EcoStruxure Hybrid Distributed Control System (DCS)
EcoStruxure Machine Expert (SoMachine)
EcoStruxure Machine Expert Basic
EcoStruxure Operator Terminal Expert
Facility Expert Online
EcoStruxure Power Monitoring Expert
EcoStruxure Power SCADA Operation (PowerSCADA Expert / PowerLogic SCADA)
Eurotherm Data Reviewer
Eurotherm iTools
eXLhoist Configuration Software
Schneider Electric License Manager
Harmony XB5SSoft
SoMachine Motion
SoMove
Versatile Software BLUE
Vijeo Designer
OsiSense XX Configuration Software
Zelio Soft 2

Následky

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

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-2020-196-01_SESU_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-196-01 https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-196-02_Schneider_Electric_Floating_License_Manager_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-196-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP produkty - viacero zraniteľností

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.05.2020

CVE

CVE-2020-6222, CVE-2020-6267, CVE-2020-6276, CVE-2020-6278, CVE-2020-6280, CVE-2020-6281, CVE-2020-6282, CVE-2020-6285, CVE-2020-6286

Zasiahnuté systémy

SAP Business Client, verzia - 6.5
SAP NetWeaver (XML Toolkit for JAVA); verzie - ENGINEAPI 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
SAP Disclosure Management; verzia - 1.0
SAP Business Objects Business Intelligence Platform (BI Launchpad); verzia - 4.2
SAP Business Objects Business Intelligence Platform (bipodata); verzia - 4.2
SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE); verzie - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS); verzie - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
SAP Business Objects Business Intelligence Platform (BI Launchpad and CMC); verzie - 4.1, 4.2
SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface) , verzie - 4.1, 4.2
SAP NetWeaver (ABAP Server) and ABAP Platform; verzie - 731, 740, 750

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-sap-products-could-allow-for-arbitrary-code-execution_2020-93/

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

Identifikátor

Capsule Technologies SmartLinx Neuron 2 - zraniteľnosť

Popis

Spoločnosť Capsule Technologies vydala bezpečnostnú aktualizáciu na svoj produkt SmartLinx Neuron 2, ktorá opravuje kritickú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi s fyzickým prístupom k USB portu zariadenia prevziať kontrolu nad systémom.

Dátum prvého zverejnenia varovania

14.07.2020

CVE

CVE-2019-5024

Zasiahnuté systémy

Capsule Technologies SmartLinx Neuron 2 verzie staršie ako 9.0

Následky

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

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-20-196-01

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

Identifikátor

Apache Tomcat - viacero zraniteľností

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Tomcat, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

14.07.2020

CVE

CVE-2020-13934, CVE-2020-13935

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 10.0.0-M7
Apache Tomcat verzie staršie ako 9.0.37
Apache Tomcat verzie staršie ako 8.5.57

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

http://mail-archives.us.apache.org/mod_mbox/www-announce/202007.mbox/%3C39e4200c-6f4e-b85d-fe4b-a9c2bd5fdc3d%40apache.org%3E
http://mail-archives.us.apache.org/mod_mbox/www-announce/202007.mbox/%3Cad62f54e-8fd7-e326-25f1-3bdf1ffa3818%40apache.org%3E
https://nvd.nist.gov/vuln/detail/CVE-2020-13935

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

Identifikátor

Joomla! zraniteľnosti

Popis

Vývojári systému pre správu obsahu Joomla! vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.07.2019

CVE

CVE-2020-15695, CVE-2020-15696, CVE-2020-15697, CVE-2020-15698, CVE-2020-15699, CVE-2020-15700

Zasiahnuté systémy

Joomla! CMS verzie staršie ako 3.9.20

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Joomla! v zraniteľnej verzii. V prípade že áno, zabezpečte aktualizáciu redakčného systému.
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://developer.joomla.org/security-centre/818-20200701-core-csrf-in-com-installer-ajax-install-endpoint.html
https://developer.joomla.org/security-centre/822-20200705-core-escape-mod-random-image-link.html
https://developer.joomla.org/security-centre/820-20200703-core-csrf-in-com-privacy-remove-request-feature.html
https://developer.joomla.org/security-centre/819-20200702-core-missing-checks-can-lead-to-a-broken-usergroups-table-record.html
https://developer.joomla.org/security-centre/823-20200706-core-system-information-screen-could-expose-redis-or-proxy-credentials.html
https://nvd.nist.gov/vuln/detail/CVE-2020-15700
https://nvd.nist.gov/vuln/detail/CVE-2020-15697
https://nvd.nist.gov/vuln/detail/CVE-2020-15698
https://nvd.nist.gov/vuln/detail/CVE-2020-15699
https://nvd.nist.gov/vuln/detail/CVE-2020-15695
https://nvd.nist.gov/vuln/detail/CVE-2020-15696

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-185