BEZPEČNOSTNÝ BULLETIN

Týždeň 12. 08. 2020 - 18. 08. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe produkty - viacero zraniteľností	Vysoká	**8.8**
02.	Apple iCloud - viacero zraniteľností	Vysoká	**8.8**
03.	Parallels Desktop for Mac - viacero zraniteľností	Vysoká	**8.8**
04.	Yokogawa CENTUM - viacero zraniteľností	Vysoká	**8.1**
05.	Apache Struts - viacero zraniteľností	Vysoká	**8.1**
06.	IBM WebSphere - bezpečnostná zraniteľnosť	Vysoká	**8.1**
07.	Zoom - viacero zraniteľností	Stredná	**6.5**
08.	TinyMCE - bezpečnostná zraniteľnosť	Stredná	**6.1**

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-206

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 svoje produkty Lightroom, Acrobat a Acrobat Reader, 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

11.08.2020

CVE

CVE-2020-9693, CVE-2020-9694, CVE-2020-9695, CVE-2020-9696, CVE-2020-9697, CVE-2020-9698, CVE-2020-9699, CVE-2020-9700, CVE-2020-9701, CVE-2020-9702, CVE-2020-9703, CVE-2020-9704, CVE-2020-9705, CVE-2020-9706, CVE-2020-9707, CVE-2020-9710, CVE-2020-9711, CVE-2020-9712, CVE-2020-9713, CVE-2020-9714, CVE-2020-9715, CVE-2020-9716, CVE-2020-9717, CVE-2020-9718, CVE-2020-9719, CVE-2020-9720, CVE-2020-9721, CVE-2020-9722, CVE-2020-9723, CVE-2020-9724

Zasiahnuté systémy

Adobe Lightroom Classic verzie staršie ako 9.3
Acrobat DC verzie staršie ako 2020.012.20041
Acrobat Reader DC verzie staršie ako 2020.012.20041
Acrobat 2020 verzie staršie ako 2020.001.30005
Acrobat Reader 2020 verzie staršie ako 2020.001.30005
Acrobat 2017 verzie staršie ako 2017.011.30175
Acrobat Reader 2017 verzie staršie ako 2017.011.30175
Acrobat 2015 verzie staršie ako 2015.006.30527
Acrobat Reader 2015 verzie staršie ako 2015.006.30527

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/acrobat/apsb20-48.html
https://helpx.adobe.com/security/products/lightroom/apsb20-51.html
https://threatpost.com/critical-adobe-acrobat-reader-bugs-rce/158261/
https://www.securityweek.com/adobe-patches-11-critical-vulnerabilities-acrobat-and-reader

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

Identifikátor

Apple iCloud - viacero zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoj produkt iCloud, ktorá opravuje 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

10.08.2020

CVE

CVE-2020-9862, CVE-2020-9871, CVE-2020-9872, CVE-2020-9873, CVE-2020-9874, CVE-2020-9875, CVE-2020-9876, CVE-2020-9877, CVE-2020-9879, CVE-2020-9893, CVE-2020-9894, CVE-2020-9895, CVE-2020-9910, CVE-2020-9915, CVE-2020-9916, CVE-2020-9919, CVE-2020-9925, CVE-2020-9936, CVE-2020-9937, CVE-2020-9938

Zasiahnuté systémy

iCloud for Windows verzie staršie ako 11.3 a 7.20

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
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://support.apple.com/sk-sk/HT211295
https://support.apple.com/sk-sk/HT211294

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

Identifikátor

Parallels Desktop for Mac - viacero zraniteľností

Popis

Vývojári Parallels Desktop for Mac vydali aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.08.2020

CVE

CVE-2020-17390, CVE-2020-17391, CVE-2020-17392, CVE-2020-17393, CVE-2020-17394, CVE-2020-17395, CVE-2020-17396, CVE-2020-17397, CVE-2020-17398, CVE-2020-17399, CVE-2020-17400, CVE-2020-17401, CVE-2020-17402

Zasiahnuté systémy

Parallels Desktop for Mac verzie staršie ako 16.0.0 (48916)

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.parallels.com/en/125013
https://www.zerodayinitiative.com/advisories/ZDI-20-1011/
https://www.zerodayinitiative.com/advisories/ZDI-20-1012/
https://www.zerodayinitiative.com/advisories/ZDI-20-1013/
https://www.zerodayinitiative.com/advisories/ZDI-20-1014/
https://www.zerodayinitiative.com/advisories/ZDI-20-1015/
https://www.zerodayinitiative.com/advisories/ZDI-20-1016/
https://www.zerodayinitiative.com/advisories/ZDI-20-1017/
https://www.zerodayinitiative.com/advisories/ZDI-20-1018/
https://www.zerodayinitiative.com/advisories/ZDI-20-1019/
https://www.zerodayinitiative.com/advisories/ZDI-20-1020/
https://www.zerodayinitiative.com/advisories/ZDI-20-1008/
https://www.zerodayinitiative.com/advisories/ZDI-20-1009/
https://www.zerodayinitiative.com/advisories/ZDI-20-1010/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Yokogawa CENTUM - viacero zraniteľností

Popis

Spoločnosť Yokogawa vydala bezpečnostné aktualizácie na svoj produkt CENTUM, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.08.2020

CVE

CVE-2020-5608, CVE-2020-5609

Zasiahnuté systémy

Yokogawa CENTUM VP R5.01.00 – R5.04.20 verzie staršie ako patch R5.04.D1
Yokogawa CENTUM VP R6.01.00 – R6.07.00 verzie staršie ako patch R6.07.11
B/M9000CS verzie R5.04.01 - R5.05.01
B/M9000VP verzie R6.01.01 - R8.03.01

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://us-cert.cisa.gov/ics/advisories/icsa-20-224-01
https://www.ptsecurity.com/ww-en/about/news/positive-technologies-helps-eliminate-vulnerabilities-in-yokogawas-centum-dcs-distributed-control-system/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Struts - viacero zraniteľností

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Struts, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedené zraniteľnosti je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

13.08.2020

CVE

CVE-2019-0230, CVE-2019-0233

Zasiahnuté systémy

Apache Struts verzie staršie ako 2.5.22

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame bezodkladne nainštalovať bezpečnostné aktualizácie.
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

http://mail-archives.us.apache.org/mod_mbox/www-announce/202008.mbox/%3C66006167-999e-a1e5-4a3a-5f1c75a1e8a2%40apache.org%3E
https://www.tenable.com/blog/cve-2019-0230-apache-struts-potential-remote-code-execution-vulnerability
https://www.helpnetsecurity.com/2020/08/17/cve-2019-0230/
https://access.redhat.com/security/cve/cve-2019-0233
https://access.redhat.com/security/cve/cve-2019-0230

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM WebSphere - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje produkty IBM WebSphere, ktoré opravujú bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.08.2020

CVE

CVE-2020-4589

Zasiahnuté systémy

IBM WebSphere Application Server a WebSphere Application Server Hypervisor Edition verzie staršie ako 9.0.5.5, 8.5.5.18, 8.0.0.15 7.0.0.45 a Interim Fix PH27414

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.ibm.com/support/pages/security-bulletin-websphere-application-server-vulnerable-remote-code-execution-vulnerability-cve-2020-4589
https://www.cisecurity.org/advisory/a-vulnerability-in-ibm-websphere-application-server-could-allow-for-remote-code-execution_2020-117/
https://exchange.xforce.ibmcloud.com/vulnerabilities/184585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4589

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zoom - viacero zraniteľností

Popis

Spoločnosť Zoom vydala bezpečnostnú aktualizáciu na svoj produkt Zoom, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.08.2020

CVE

-

Zasiahnuté systémy

Zoom verzie staršie ako 5.2.0

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.zoom.us/hc/en-us/articles/201361953-New-updates-for-Windows
https://www.darkreading.com/application-security/zoom-vulnerabilities-demonstrated-in-def-con-talk/d/d-id/1338636

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TinyMCE - bezpečnostná zraniteľnosť

Popis

Vývojári HTML textového editora TinyMCE vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.08.2020

CVE

CVE-2020-12648

Zasiahnuté systémy

TinyMCE verzie staršie ako 4.9.11 a 5.4.1

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky neobsahujú HTML textový editor TinyMCE v zraniteľnej verzii. V prípade že áno, zabezpečte jeho aktualizáciu.
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://www.securityweek.com/potentially-serious-vulnerability-found-popular-wysiwyg-editor-tinymce
https://github.com/tinymce/tinymce/security/advisories/GHSA-vrv8-v4w8-f95h
https://labs.bishopfox.com/advisories/tinymce-version-5.2.1