BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 06. 2022 - 21. 06. 2022

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:
01794/2022/SK-CERT-793

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

Identifikátor

Virtualizačný hypervízor Xen - viacero bezpečnostných zraniteľností

Popis

Vývojári hypervízora Xen vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených vstupov eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.09.2022

CVE

CVE-2022-26362, CVE-2022-26363, CVE-2022-26364

Zasiahnuté systémy

Xen vo verzii staršej ako 4.16

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://vuldb.com/?id.201537
http://xenbits.xen.org/xsa/advisory-401.html
https://www.theregister.com/2022/06/14/xen_guest_escape_flaws/
https://nvd.nist.gov/vuln/detail/CVE-2022-26363
https://www.securitynewspaper.com/2022/06/14/3-critical-vulnerabilities-in-xen-project-allows-to-take-control-of-host-os-via-vms-in-x86-pv/

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

Identifikátor

ABB produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoje produkty ABB Automation Builder, Drive Composer a Mint WorkBench, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.06.2022

CVE

CVE-2022-26057, CVE-2022-31216, CVE-2022-31217, CVE-2022-31218, CVE-2022-31219

Zasiahnuté systémy

Drive Compose entry vo verziách 2.0 až 2.7
Drive Composer pro vo verziách 2.0 až 2.7
ABB Automation Builder 1.1.0 až 2.5.0
Mint WorkBench build 5866 a staršie

Následky

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

Odporúčania

Administrátorom a používateľom 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://nvd.nist.gov/vuln/detail/CVE-2022-31216
https://vuldb.com/?id.202196
https://search.abb.com/library/Download.aspx?DocumentID=9AKK108467A0305&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.38192870.478847987.1655218701-372504397.1647012599

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoje portfólio produktov Adobe Animate, Bridge, Illustrator, Incopy,InDesign, a RoboHelp, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.06.2022

CVE

CVE-2022-28839, CVE-2022-28840, CVE-2022-28841, CVE-2022-28842, CVE-2022-28843, CVE-2022-28844, CVE-2022-28845, CVE-2022-28846, CVE-2022-28847, CVE-2022-28848, CVE-2022-28849, CVE-2022-28850, CVE-2022-30637, CVE-2022-30638, CVE-2022-30639, CVE-2022-30640, CVE-2022-30641, CVE-2022-30642, CVE-2022-30643, CVE-2022-30644, CVE-2022-30645, CVE-2022-30646, CVE-2022-30647, CVE-2022-30648, CVE-2022-30649, CVE-2022-30650, CVE-2022-30651, CVE-2022-30652, CVE-2022-30653, CVE-2022-30654, CVE-2022-30655, CVE-2022-30656, CVE-2022-30657, CVE-2022-30658, CVE-2022-30659, CVE-2022-30660, CVE-2022-30661, CVE-2022-30662, CVE-2022-30663, CVE-2022-30664, CVE-2022-30665, CVE-2022-30666, CVE-2022-30667, CVE-2022-30668, CVE-2022-30669, CVE-2022-30670

Zasiahnuté systémy

Adobe Animate, Bridge, Illustrator, Incopy,InDesign, a RoboHelp
Úplný zoznam zraniteľných verzií možno nájsť na https://helpx.adobe.com/security/security-bulletin.html

Následky

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

Odporúčania

Administrátorom a používateľom 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://helpx.adobe.com/security/security-bulletin.html

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

Identifikátor

Microsoft Office - Follina - viacero kritických bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na operačné systémy Windows, ktorá opravuje viacero kritických bezpečnostných zraniteľností vrátane aktívne zneužívanej zraniteľnosti MSDT s označením Follina.

Najzávažnejšia zraniteľnosť Follina využíva mechaniku "diag tool" na zavolanie škodlivého kódu po otvorení dokumentu v MS Office a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.06.2022

CVE

CVE-2022-30139, CVE-2022-30141, CVE-2022-30143, CVE-2022-30146, CVE-2022-30149, CVE-2022-30153, CVE-2022-30161, CVE-2022-30190

Zasiahnuté systémy

Všetky verzie MS Windows pred bezpečnostnou aktualizáciou z 30. Marca 2022

Následky

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

Odporúčania

Administrátorom a používateľom 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://docs.microsoft.com/en-us/windows/release-health/windows11-release-information
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
https://www.sk-cert.sk/sk/varovanie-pred-zneuzivanim-0-day-zranitelnosti-v-microsoft-office-word-ms-msdt-follina/

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

Identifikátor

Guzzle PHP HTTP klient - dve kritické bezpečnostné zraniteľnosti

Popis

Vývojári PHP HTTP klienta Guzzle vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom. Guzzle je používané aj v rámci jadra redakčného systému Drupal.

Dátum prvého zverejnenia varovania

09.06.2022

CVE

CVE-2022-31042, CVE-2022-31043

Zasiahnuté systémy

Guzzle vo verzii staršej ako 7.4.4
Guzzle vo verzii staršej ako 6.5.7

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú knižnicu Guzzle v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://nvd.nist.gov/vuln/detail/CVE-2022-31043
https://www.drupal.org/sa-core-2022-011
https://github.com/guzzle/guzzle/security/advisories/GHSA-w248-ffj2-4v5q

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zoom produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoom Video Communications vydala bezpečnostné aktualizácie na konferenčné nástroje Zoom Client for Meetings a All Zoom Rooms for Conference Room, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorenej DLL vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.06.2022

CVE

CVE-2022-22788, CVE-2022-28749

Zasiahnuté systémy

Zoom Client for Meetings pre Windows vo verzii staršej ako 5.10.3
All Zoom Rooms for Conference Room pre Windows vo verzii staršej ako 5.10.3

Následky

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

Odporúčania

Administrátorom a používateľom 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://explore.zoom.us/en/trust/security/security-bulletin/
https://nvd.nist.gov/vuln/detail/CVE-2022-22788
https://vuldb.com/?id.202211