BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 07. 2022 - 19. 07. 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-829

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v Microsoft Windows Graphics spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.07.2022

CVE

CVE-2022-21845, CVE-2022-22022, CVE-2022-22023, CVE-2022-22024, CVE-2022-22026, CVE-2022-22027, CVE-2022-22028, CVE-2022-22029, CVE-2022-22031, CVE-2022-22034, CVE-2022-22036, CVE-2022-22037, CVE-2022-22038, CVE-2022-22039, CVE-2022-22040, CVE-2022-22041, CVE-2022-22042, CVE-2022-22043, CVE-2022-22045, CVE-2022-22047, CVE-2022-22048, CVE-2022-22049, CVE-2022-22050, CVE-2022-22711, CVE-2022-2294, CVE-2022-2295, CVE-2022-23816, CVE-2022-23825, CVE-2022-27776, CVE-2022-30181, CVE-2022-30187, CVE-2022-30202, CVE-2022-30203, CVE-2022-30205, CVE-2022-30206, CVE-2022-30209, CVE-2022-30211, CVE-2022-30212, CVE-2022-30213, CVE-2022-30214, CVE-2022-30215, CVE-2022-30216, CVE-2022-30220, CVE-2022-30221, CVE-2022-30222, CVE-2022-30223, CVE-2022-30224, CVE-2022-30225, CVE-2022-30226, CVE-2022-33632, CVE-2022-33633, CVE-2022-33637, CVE-2022-33641, CVE-2022-33642, CVE-2022-33643, CVE-2022-33644, CVE-2022-33650, CVE-2022-33651, CVE-2022-33652, CVE-2022-33653, CVE-2022-33654, CVE-2022-33655, CVE-2022-33656, CVE-2022-33657, CVE-2022-33658, CVE-2022-33659, CVE-2022-33660, CVE-2022-33661, CVE-2022-33662, CVE-2022-33663, CVE-2022-33664, CVE-2022-33665, CVE-2022-33666, CVE-2022-33667, CVE-2022-33668, CVE-2022-33669, CVE-2022-33671, CVE-2022-33672, CVE-2022-33673, CVE-2022-33674, CVE-2022-33675, CVE-2022-33676, CVE-2022-33677, CVE-2022-33678

Zasiahnuté systémy
AMD CPU Branch Azure Site Recovery Azure Storage Library Microsoft Defender for Endpoint Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Open Source Software Role: DNS Server Role: Windows Fax Service Role: Windows Hyper-V Skype for Business and Microsoft Lync Windows Active Directory Windows Advanced Local Procedure Call Windows BitLocker Windows Boot Manager Windows Client/Server Runtime Subsystem Windows Connected Devices Platform Service Windows Credential Guard Windows Media Windows Network File System Windows Performance Counters Windows Point-to-Point Tunneling Protocol Windows Portable Device Enumerator Service Windows Print Spooler Components Windows Remote Procedure Call Runtime Windows Security Account Manager Windows Server Service Windows Shell Windows Storage XBox Presnú špecifikáciu zasiahnutých produktov nájdete na webovej adrese: https://msrc.microsoft.com/update-guide/releaseNote/2022-Jul

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://msrc.microsoft.com/update-guide/releaseNote/2022-Jul

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte SAP BusinessObjects Business Intelligence Platform spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-28771, CVE-2022-29619, CVE-2022-31591, CVE-2022-31592, CVE-2022-31593, CVE-2022-31597, CVE-2022-31598, CVE-2022-32246, CVE-2022-32247, CVE-2022-32248, CVE-2022-32249, CVE-2022-35168, CVE-2022-35169, CVE-2022-35170, CVE-2022-35171, CVE-2022-35172, CVE-2022-35224, CVE-2022-35225, CVE-2022-35227, CVE-2022-35228

Zasiahnuté systémy

Product-SAP BusinessObjects vo verzii staršej ako (vrátane)s -420, 430
Product-SAP Business One, vo verzii staršej ako (vrátane) -10.0
Product-SAP BusinessObjects 4.x,vo verzii staršej ako (vrátane) -420, 430
Product-SAPS/4HANA,vo verzii staršej ako (vrátane)s -104, 105, 106
Product-SAP NetWeaver Application Server for ABAP and ABAP Platform,vo verzii staršej ako (vrátane) -700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
Product-SAP NetWeaver Enterprise Portal, vo verzii staršej ako (vrátane) -7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
Product-SAP Enterprise Portal, vo verzii staršej ako (vrátane) -7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50
Product-SAP Enterprise Extension Defense Forces & Public Security (EA-DFPS),vo verzii staršej ako (vrátane) -605, 606, 616,617,618, 802, 803, 804, 805, 806
Product-SAP3D Visual Enterprise Viewer, vo verzii staršej ako (vrátane) -9.0
Product-SAP Adaptive Server Enterprise (ASE),vo verzii staršej ako (vrátane) -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do 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://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

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 bezpečnostné aktualizácie na produkty Acrobat, Acrobat Reader, RoboHelp, Character Animator a Photoshop, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti nachádzajúce sa v produktoch Acrobat, Acrobat Reader, Character Animation a Photoshop spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-23201, CVE-2022-34215, CVE-2022-34216, CVE-2022-34217, CVE-2022-34219, CVE-2022-34220, CVE-2022-34221, CVE-2022-34222, CVE-2022-34223, CVE-2022-34224, CVE-2022-34225, CVE-2022-34226, CVE-2022-34227, CVE-2022-34228, CVE-2022-34229, CVE-2022-34230, CVE-2022-34232, CVE-2022-34233, CVE-2022-34234, CVE-2022-34236, CVE-2022-34237, CVE-2022-34238, CVE-2022-34239, CVE-2022-34241, CVE-2022-34242, CVE-2022-34243, CVE-2022-34244

Zasiahnuté systémy

Acrobat a Reader vo verzii staršej ako 22.001.20169, 20.005.30362 a 17.012.30249
RoboHelp vo verzii staršej ako RH2020.0.8
Character Animator 2021 vo vezii staršej ako 4.4.8
Character Animator 2022 vo verzii staršej ako 22.4
Photoshop vo verzii staršej ako 22.5.8 a 23.4.1

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://helpx.adobe.com/security/products/robohelp/apsb22-10.html
https://helpx.adobe.com/security/products/acrobat/apsb22-32.html
https://helpx.adobe.com/security/products/character_animator/apsb22-34.html
https://helpx.adobe.com/security/products/photoshop/apsb22-35.html

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

Identifikátor

Lenovo Notebook BIOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu firmwaru svojich notebookov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-1890, CVE-2022-1891, CVE-2022-1892

Zasiahnuté systémy

Notebooky Lenovo, presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://support.lenovo.com/sk/en/product_security/len-91369

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu firmwaru 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.lenovo.com/sk/en/product_security/len-91369

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

xorg-x11-server - dve bezpečnostné zraniteľnosti

Popis

Vývojári open source implementácie zobrazovacieho servera X Window System X.Org Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-2319, CVE-2022-2320

Zasiahnuté systémy

xorg-server vo verzii staršej ako 21.1.4

Následky

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

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://www.cybersecurity-help.cz/vdb/SB2022071309
https://www.phoronix.com/scan.php?page=news_item&px=X.Org-July-12-Security
https://lists.x.org/archives/xorg/2022-July/061035.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware vRealize, vCenter a ESXi - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty vRealize, vCenter Server, Cloud Foundation a ESXi, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v produkte ESXi spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora získať neoprávnený prístup k citlivým údajom vo VM (Virtual Machine) prevádzkovaných na rovnakom ESXi hoste.

Dátum prvého zverejnenia varovania

12.07.2022

CVE

CVE-2022-22982, CVE-2022-23816, CVE-2022-28693, CVE-2022-29901, CVE-2022-31654, CVE-2022-31655

Zasiahnuté systémy

VMware ESXi vo verzii staršej ako ESXi70U3sf-20036586 a ESXi650-202207401-SG
VMware Cloud Foundation vo verzii staršej ako KB88695 a KB88927
VMware vRealize Log Insight vo verzii staršej ako 8.8.2
VMware vCenter Server vo verzii staršej ako 7.0 U3f, 6.7 U3r a 6.5 U3t
VMware Cloud Foundation vo verzii staršej ako KB88287

Následky

Neoprávnený prístup k citlivým údajom

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://www.vmware.com/security/advisories/VMSA-2022-0020.html
https://www.vmware.com/security/advisories/VMSA-2022-0019.html
https://www.vmware.com/security/advisories/VMSA-2022-0018.html