BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 07. 2021 - 20. 07. 2021

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:
01439/2020/SK-CERT-490

BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 07. 2021 - 20. 07. 2021

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.07.2021

CVE

CVE-2021-28591, CVE-2021-28592, CVE-2021-28593, CVE-2021-28595, CVE-2021-28596, CVE-2021-28624, CVE-2021-28634, CVE-2021-28635, CVE-2021-28636, CVE-2021-28637, CVE-2021-28638, CVE-2021-28639, CVE-2021-28640, CVE-2021-28641, CVE-2021-28642, CVE-2021-28643, CVE-2021-28644, CVE-2021-35980, CVE-2021-35981, CVE-2021-35983, CVE-2021-35984, CVE-2021-35985, CVE-2021-35986, CVE-2021-35987, CVE-2021-35988, CVE-2021-35989, CVE-2021-35990, CVE-2021-35991, CVE-2021-35992, CVE-2021-36008, CVE-2021-36009, CVE-2021-36010

Zasiahnuté systémy

Adobe Dimension vo verzii staršej ako 3.4.3
Adobe Illustrator 2021 vo verzii staršej ako 25.3
Adobe Framemaker 2019 vo verzii staršej ako Release Update 8 (hotfix)
Adobe Framemaker 2020 vo verzii staršej ako Release Update 2
Acrobat DC vo verzii staršej ako 2021.005.20058
Acrobat 2020 vo verzii staršej ako 2020.004.30006
Acrobat 2017 vo verzii staršej ako 2017.011.30199
Acrobat Reader 2017 vo verzii staršej ako 2017.011.30199

Následky

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

Odporúčania

Administrátorom a používateľom 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://helpx.adobe.com/security.html/security/security-bulletin.ug.html
https://helpx.adobe.com/security/products/dimension/apsb21-40.html
https://helpx.adobe.com/security/products/illustrator/apsb21-42.html
https://helpx.adobe.com/security/products/framemaker/apsb21-45.html
https://helpx.adobe.com/security/products/acrobat/apsb21-51.html
https://helpx.adobe.com/security/products/bridge/apsb21-53.html
https://threatpost.com/adobe-patches-critical-acrobat/167743/
https://www.bleepingcomputer.com/news/security/adobe-updates-fix-28-vulnerabilities-in-6-programs/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WooCommerce wordpress plugin - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu WooCommerce vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

13.07.2021

CVE

-

Zasiahnuté systémy

WooCommerce plugin vo verzii staršej ako 5.5.1
WooCommerce Blocks vo verzii staršej ako 5.5.1

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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.
Pri webových stránkach odporúčame zvážiť možnosť prevádzkovať redakčný systém nedostupný z verejného internetu a na verejný prezentačný server nahrávať len vyexportovanú statickú verziu stránky.

Zdroje

https://threatpost.com/zero-day-attacks-woocommerce-databases/167846/
https://www.wordfence.com/blog/2021/07/critical-sql-injection-vulnerability-patched-in-woocommerce/
https://woocommerce.com/posts/critical-vulnerability-detected-july-2021/#
https://twitter.com/thedawgyg/status/1415479999705096194
https://www.securityweek.com/critical-woocommerce-vulnerability-targeted-hours-after-patch
https://patchstack.com/woocommerce-sql-injection-vulnerability/
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.07.2021

CVE

CVE-2020-15782, CVE-2020-28400, CVE-2021-27387, CVE-2021-27399, CVE-2021-31895, CVE-2021-34326, CVE-2021-34327, CVE-2021-34328, CVE-2021-34329

Zasiahnuté systémy

RUGGEDCOM ROS i800 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS i801 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS i802 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS i803 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS M969 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS M2100 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS M2200 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC20 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC30 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC40 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC41 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC8388 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RMC8388 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RP110 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS400 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS401 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS416 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS416V2 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS416V2 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RS900 (32M) V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS900 (32M) V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RS900G vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS900G (32M) V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS900G (32M) V5.X vo verzii staršej ako 5.5.4

RUGGEDCOM ROS RS900GP vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS900L vo verzii staršej ako 4.3.7
RUGGEDCOM ROS PS900W vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS910 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS910L vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS910W vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS920L vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS920W vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS930L vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS930W vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS940G vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS969 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS8000 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS8000A vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS8000H vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RS8000T vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG900 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG900 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG900C vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG900G V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG800G V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG900R vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG920P V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG920P V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2100 (32M) V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2100 (32M) V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2100 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2100P vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2100P (32M) V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2100P (32M) V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2200 vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2288 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2288 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2300 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2300 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2300P V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2300P V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSG2488 V4.X vo verzii staršej ako 4.3.7
RUGGEDCOM ROS RSG2488 V5.X vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RSL910 vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RST916C vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RST916P vo verzii staršej ako 5.5.4
RUGGEDCOM ROS RST2228 vo verzii staršej ako 5.5.4
SINAMICS PERFECT HARMONY GH180 všetky verzie
Simcenter Femap vo verzii staršej ako V2020.2.MP3
Simcenter Femap vo verzii staršej ako V2021.1.MP3
Solid Edge vo verzii staršej ako SE2021MP5
JT2Go vo verzii staršej ako V13.2
Teamcenter Visualization vo verzii staršej ako V13.2
RUGGEDCOM RM1224 vo verzii staršej ako v6.4

SCALANCE M-800 vo verzii staršej ako v6.4
SCALANCE S615 vo verzii staršej ako v6.4
SCALANCE W700 IEEE 802.11n všetky verzie
SCALANCE W700 IEEE 802.11ac všetky verzie
SCALANCE X200-4 P IRT vo verzii staršej ako v5.5.0
SCALANCE X201-3P IRT vo verzii staršej ako v5.5.0
SCALANCE X201-3P IRT PRO vo verzii staršej ako v5.5.0
SCALANCE X202-2 IRT vo verzii staršej ako v5.5.0
SCALANCE X202-2P IRT (vrátane SIPLUS NET variant) vo verzii staršej ako v5.5.0
SCALANCE X202-2P IRT PRO vo verzii staršej ako v5.5.0
SCALANCE X204 IRT vo verzii staršej ako v5.5.0
SCALANCE X204 IRT PRO vo verzii staršej ako v5.5.0
SCALANCE X204-2 (vrátane SIPLUS NET variant) všetky verzie
SCALANCE X204-2FM všetky verzie
SCALANCE X204-2LD (vrátane SIPLUS NET variant) všetky verzie
SCALANCE X20204-2LD TS všetky verzie
SCALANCE X204 -2TS všetky verzie
SCALANCE X206-1 všetky verzie
SCALANCE X206-1LD (vrátane SIPLUS NET variant) všetky verzie
SCALANCE X208 (vrátane SIPLUS NET variant) všetky verzie
SCALANCE X208PRO všetky verzie
SCALANCE X212-2 všetky verzie
SCALANCE X12-2LD všetky verzie
SCALANCE X216 všetky verzie
SCALANCE X224 všetky verzie
SCALANCE X302-7EEC všetky verzie
SCALANCE 304-2FE všetky verzie
SCALANCE X306-1LDFE všetky verzie
SCALANCE X307-2EEC všetky verzie
SCALANCE X307-3 všetky verzie
SCALANCE X307-3LD všetky verzie
SCALANCE X308-2 (vrátane SIPLUS NET variant) všetky verzie
SCALANCE X308-2LD všetky verzie
SCALANCE X308-2LH všetky verzie
SCALANCE X308-2LH+ všetky verzie
SCALANCE X308-2M všetky verzie
SCALANCE X308-2M POE všetky verzie
SCALANCE X308-2M TS všetky verzie
SCALANCE X310 všetky verzie
SCALANCE X310FE všetky verzie
SCALANCE X320-1FE všetky verzie
SCALANCE X320-3LDFE všetky verzie
SCALANCE XB-200 všetky verzie
SCALANCE XC-200 všetky verzie
SCALANCE XF201-3P IRT vo verzii staršej ako v5.5.0
SCALANCE XF202-2P IRT vo verzii staršej ako v5.5.0
SCALANCE XF204 všetky verzie
SCALANCE XF204 IRT vo verzii staršej ako v5.5.0
SCALANCE XF204-2 (vrátane SIPLUS NET variant) všetky verzie
SCALANCE XF204-2BA IRT vo verzii staršej ako v5.5.0

SCALANCE XF206-1 všetky verzie
SCALANCE XF208 všetky verzie
SCALANCE XF-200BA všetky verzie
SCALANCE XM400 vo verzii staršej ako v6.3.1
SCALANCE XP-200 všetky verzie
SCALANCE XR324-4M EEC všetky verzie
SCALANCE XR324-4M POE všetky verzie
SCALANCE XR324-4M POE TS všetky verzie
SCALANCE XR324-12M všetky verzie
SCALANCE XR324-12M TS všetky verzie
SCALANCE XR500 vo verzii staršej ako v6.3.1
SCALANCE XR-300WG všetky verzie
SIMATIC CFU PA všetky verzie
SIMATIC IE/PB-LINK V3 všetky verzie
SIMATIC MV500 family vo verzii staršej ako v3.0
SIMATIC NET CM 1542-1 všetky verzie
SIMATIC NET CP1616/CP1604 vo verzii staršej ako 2.7 (vrátane)
SIMATIC NET CP1626 všetky verzie
SIMATIC NET DK-16xx PN IO vo verzii staršej ako 2.7 (vrátane)
SIMATIC Power Line Booster PLB, Base Module (MLFB: 6ES7972-5AA10-0AB0) všetky verzie
SIMATIC PROFINET Driver všetky verzie
SIMATIC S7-1200 CPU family (vrátane SIPLUS variants SIPLUS variants) vo verzii staršej ako v4.5
SIMOCODE proV Ethernet/IP vo verzii staršej ako v1.1.3
SIMOCODE proV PROFINET vo verzii staršej ako v2.1.3
SOFTNET-IE PNIO všetky verzie
SIMATIC PCS 7 všetky verzie
SIMATIC PCS 7 vo verzii staršej ako V9.0 SP3
SIMATIC PDM vo verzii staršej ako V9.2
SIMATIC STEP 7 vo verzii staršej ako V5.6 SP2 HF3
SINAMICS STARTER vo verzii staršej ako V5.4 HF2

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://cert-portal.siemens.com/productcert/pdf/ssa-373591.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-434535.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-434536.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-133038.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-173615.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-483182.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-599968.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-641963.pdf
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-10

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

Identifikátor

Microsoft Windows Print Spooler - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na produkt Windows Print Spooler, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.07.2021

CVE

CVE-2021-34481

Zasiahnuté systémy
Microsoft Windows Server 2008 SP2 x32 Microsoft Windows Server 2008 SP2 x64 Microsoft Windows 7 SP1 x32 Microsoft Windows 7 SP1 x64 Microsoft Windows Server 2012 Microsoft Windows 8.1 x32 Microsoft Windows 8.1 x64 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows 10 1809 pre x64-based Systems Microsoft Windows 10 1809 pre 32-bit Systems Microsoft Windows 10 1803 pre 32-bit Systems Microsoft Windows 10 1803 pre x64-based Systems Microsoft Windows 10 1803 pre ARM64-based Systems Microsoft Windows 10 1809 pre ARM64-based Systems Microsoft Windows 10 2004 pre 32-bit Systems Microsoft Windows 10 2004 pre ARM64-based Systems Microsoft Windows 10 2004 pre x64-based Systems Microsoft Windows 10 1909 pre 32-bit Systems Microsoft Windows 10 1909 pre x64-based Systems Microsoft Windows 10 1909 pre ARM64-based Systems Microsoft Windows 10 20H2 pre 32-bit Systems Microsoft Windows 10 20H2 pre ARM64-based Systems Microsoft Windows 10 20H2 pre x64-based Systems Microsoft Windows Server (Server Core installation) 2019 Microsoft Windows Server (Server Core installation) 1909 Microsoft Windows Server (Server Core installation) 2004 Microsoft Windows Server (Server Core installation) 20H2 Microsoft Windows Server (Server Core installation) 2016 Microsoft Windows Server (Server Core installation) 2012 R2 Microsoft Windows Server (Server Core installation) 2012 Microsoft Windows Server pre X64-based systems (Server Core installation) 2008 R2 Microsoft Windows Server pre X64-based systems (Server Core installation) 2008 SP2 Microsoft Windows 10 21H1 pre 32-bit Systems Microsoft Windows 10 21H1 pre ARM64-based Systems Microsoft Windows 10 21H1 pre x64-based Systems Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34481

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

Odporúčania
Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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. Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje
https://threatpost.com/microsoft-unpatched-bug-windows-print-spooler/167855/ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34481 https://www.bleepingcomputer.com/news/microsoft/new-windows-print-spooler-zero-day-exploitable-via-remote-print-servers/

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

Identifikátor

Microsoft Windows 10 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Microsoft Windows 10.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.07.2021

CVE

CVE-2021-36934

Zasiahnuté systémy

Microsoft Windows 10 1809
Microsoft Windows 10 1909
Microsoft Windows 10 20H2
Microsoft Windows 10 21H1
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame obmedziť prístup k obsahu priečinku %windir%\system32\config.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/vulnerability/CVE-2021-36934
https://therecord.media/serioussam-bug-impacts-all-windows-10-versions-released-in-the-past-2-5-years/
https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/
https://twitter.com/gentilkiwi/status/1417229454305267714
https://twitter.com/gentilkiwi/status/1417235569718013954
https://twitter.com/GossiTheDog/status/1417258450049015809
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
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 spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.07.2021

CVE

CVE-2021-27604, CVE-2021-33667, CVE-2021-33670, CVE-2021-33671, CVE-2021-33676, CVE-2021-33677, CVE-2021-33678, CVE-2021-33680, CVE-2021-33681, CVE-2021-33682, CVE-2021-33683, CVE-2021-33684, CVE-2021-33687, CVE-2021-33689

Zasiahnuté systémy

SAP NetWeaver Guided Procedures (Administration Workset)
SAP NetWeaver AS pre Java (Http Service)
SAP CRM
SAP Process Integration (Enterprise Service Repository JAVA Mappings)
SAP NetWeaver AS ABAP and ABAP Platprem
SAP NetWeaver AS ABAP (Reconciliation Framework)
SAP Lumira Server
SAP Web Dispatcher and Internet Communication Manager
SAP NetWeaver AS JAVA (Enterprise Portal)
SAP Business Objects Web Intelligence (BI Launchpad)
SAP 3D Visual Enterprise Viewer
SAP NetWeaver AS JAVA (Administrator applications)
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=580617506

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=580617506

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware ESXi a Cloud Foundation - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na produkty ESXi a Cloud Foundation, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.07.2021

CVE

CVE-2021-21994, CVE-2021-21995

Zasiahnuté systémy

ESXi 7.0 vo verzii staršej ako ESXi70U2-17630552
ESXi 6.7 vo verzii staršej ako ESXi670-202103101-SG
ESXi 6.5 vo verzii staršej ako ESXi650-202107401-SG
Cloud Foundation (ESXi) 4.x všetky verzie
Cloud Foundation (ESXi) 3.x vo verzii staršej ako 3.10.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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-2021-0014.html
https://www.securityweek.com/vmware-patches-vulnerabilities-esxi-thinapp
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L

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-490