BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 11. 2022 - 15. 11. 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-939

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 portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v Microsoft Exchange Server, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.11.2022

CVE

CVE-2022-23824, CVE-2022-3602, CVE-2022-3786, CVE-2022-37966, CVE-2022-37967, CVE-2022-37992, CVE-2022-38014, CVE-2022-38015, CVE-2022-38023, CVE-2022-39253, CVE-2022-39327, CVE-2022-41039, CVE-2022-41044, CVE-2022-41045, CVE-2022-41047, CVE-2022-41048, CVE-2022-41049, CVE-2022-41050, CVE-2022-41051, CVE-2022-41052, CVE-2022-41054, CVE-2022-41055, CVE-2022-41057, CVE-2022-41060, CVE-2022-41061, CVE-2022-41062, CVE-2022-41063, CVE-2022-41064, CVE-2022-41066, CVE-2022-41073, CVE-2022-41085, CVE-2022-41086, CVE-2022-41088, CVE-2022-41090, CVE-2022-41091, CVE-2022-41092, CVE-2022-41093, CVE-2022-41095, CVE-2022-41096, CVE-2022-41097, CVE-2022-41098, CVE-2022-41099, CVE-2022-41100, CVE-2022-41101, CVE-2022-41102, CVE-2022-41103, CVE-2022-41104, CVE-2022-41105, CVE-2022-41106, CVE-2022-41107, CVE-2022-41109, CVE-2022-41113, CVE-2022-41114, CVE-2022-41116, CVE-2022-41118, CVE-2022-41119, CVE-2022-41120, CVE-2022-41122, CVE-2022-41125, CVE-2022-41128

Zasiahnuté systémy
.NET Framework
AMD CPU Branch
Azure
Azure Real Time Operating System
Linux Kernel
Microsoft Dynamics
Microsoft Edge (Chromium-based)
Microsoft Exchange Server
Microsoft Graphics Component
Microsoft Office
Microsoft Office Excel
Microsoft Office SharePoint
Microsoft Office Word
Network Policy Server (NPS)
Open Source Software
Role: Windows Hyper-V
SysInternals
Visual Studio
Windows Advanced Local Procedure Call
Windows ALPC
Windows Bind Filter Driver
Windows BitLocker
Windows CNG Key Isolation Service
Windows Devices Human Interface
Windows Digital Media
Windows DWM Core Library
Windows Extensible File Allocation
Windows Group Policy Preference Client
Windows HTTP.sys
Windows Kerberos
Windows Mark of the Web (MOTW)
Windows Netlogon
Windows Network Address Translation (NAT)
Windows ODBC Driver
Windows Overlay Filter
Windows Point-to-Point Tunneling Protocol
Windows Print Spooler Components
Windows Resilient File System (ReFS)
Windows Scripting
Windows Win32K
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

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://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-proxynotshell-exchange-zero-days-exploited-in-attacks/ https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov

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

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje portfólio produktov ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v programe Intel® Data Center Manager (DCM), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.11.2022

CVE

CVE-2021-0185, CVE-2021-26251, CVE-2021-33064, CVE-2021-33159, CVE-2021-33164, CVE-2022-21198, CVE-2022-21794, CVE-2022-25917, CVE-2022-26006, CVE-2022-26024, CVE-2022-26028, CVE-2022-26045, CVE-2022-26047, CVE-2022-26079, CVE-2022-26086, CVE-2022-26124, CVE-2022-26341, CVE-2022-26367, CVE-2022-26369, CVE-2022-26508, CVE-2022-26513, CVE-2022-26845, CVE-2022-27187, CVE-2022-27233, CVE-2022-27497, CVE-2022-27499, CVE-2022-27638, CVE-2022-27639, CVE-2022-27874, CVE-2022-28126, CVE-2022-28611, CVE-2022-28667, CVE-2022-29466, CVE-2022-29486, CVE-2022-29515, CVE-2022-29893, CVE-2022-30297, CVE-2022-30542, CVE-2022-30548, CVE-2022-30691, CVE-2022-32569, CVE-2022-33176, CVE-2022-33942, CVE-2022-33973, CVE-2022-34152, CVE-2022-35276, CVE-2022-36349, CVE-2022-36367, CVE-2022-36370, CVE-2022-36377, CVE-2022-36380, CVE-2022-36384, CVE-2022-36400, CVE-2022-36789, CVE-2022-37334, CVE-2022-37345, CVE-2022-38099

Zasiahnuté systémy

Intel® System Studio software vo všetkých verziách
Intel® CSME vo verzii staršej ako 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25.
Intel® AMT vo verzii staršej ako 11.8.93, 11.22.93, 12.0.92, 14.1.67, 15.0.42, 16.0.
Intel® SPS vo verzii staršej ako SPS_E3_04.01.04.700.0, SPS_E3_06.00.03.035.0.
Intel® Distribution of OpenVINO™ Toolkit vo verzii staršej ako 2021.4.2.
Intel® Quartus Prime Pro edition software vo verzii staršej ako 22.1.
Intel® Quartus Prime Standard edition software vo verzii staršej ako 21.1 Patch 0.02std.
Intel® Glorp gaming particle physics demonstration software vo verzii 1.0.0.
Intel® VTune™ Profiler software vo verzii staršej ako 2022.2.0.
Intel® AMT SDK vo verzii staršej ako 16.0.4.1.
Intel® EMA vo verzii staršej ako 1.7.1.
Intel® MC vo verzii staršej ako 2.3.2.
Intel® XMM™ 7560 Modem M.2 software pre Windows alebo Linux vo verzii staršej ako M2_7560_R_01.2146.00.
Intel® PROSet/Wireless WiFi software vo verzii staršej ako 22.140.
Intel® Xeon® Processor E5 v3 Family
Intel® Xeon® Processor E5 v4 Family, Intel® Core™ X-Series Processors
11th Gen Intel® Core™ processor

Intel® Xeon® W processor
11th Gen Intel® Core™ processor family
11th Generation Intel® Core Processor Family
12th Generation Intel® Core™ Processor Family
Intel® Pentium® Gold Processor Family
Intel® Celeron® Processor Family
12th Generation Intel® Core Processor Family
10th Generation Intel® Core™ Processor Family
Intel® Core™ Processors with Intel® Hybrid Technology
Intel® Pentium® Silver N6000 Processor Family, Intel® Celeron® N4000 a N5000 Processor Families
10th Generation Intel® Core™ Processors
Intel® Xeon® W processor family
10th Gen Intel® Core™ processor
10000/1200 series
Pentium® Gold processor series
Celeron® processor 5000 series
Intel® NUC HDMI Firmware Update Tool pre NUC7i3DN, NUC7i5DN a NUC7i7DN vo verzii staršej ako 1.78.2.0.7.
Intel® SGX SDK software pre Linux vo verzii staršej ako 2.18.100.1.
Intel® SGX SDK software pre Windows vo verzii staršej ako 2.17.100.1.
Hyperscan library udržiavaná Intel®, všetky verzie stiahnuté pred 04/29/2022.
Intel® PROSet/Wireless WiFi firmware vo verzii staršej ako 22.140, Killer™ WiFi firmware vo verzii staršej ako 3.1122.3158 a UEFI vo verzii 2.2.14.22176.2.
Intel® Server Board S2600WF Family
Intel® Server Board M50CYP Family
Intel® Server Board M10JNP Family
Intel® Server System R1000WF Family
Intel® Server System R2000WF Family
Intel® SDP Tool software vo verzii staršej ako 3.0.0.
PresentMon software udržiavaná Intel® vo verzii staršej ako 1.7.1.
Intel® DCM software vo verzii staršej ako 5.0.
Intel® Advanced Link Analyzer Pro edition software vo verzii staršej ako 22.2.
Intel® Advanced Link Analyzer Standard edition software vo verzii staršej ako 22.1.1 STD.
Intel® EMA software vo verzii staršej ako 1.8.0.
Intel® WAPI Security software pre Windows 10/11 vo verzii staršej ako 22.2150.0.1.
Intel® Support Android application vo verzii staršej ako v22.02.28.
Intel® NUC 8 Rugged Kit - NUC8CCHKR
Intel® NUC Kits - NUC5PPYH, NUC5PGYH, NUC6CAYH, NUC6CAYS
Intel® NUC Board - NUC8CCHB
Intel® NUC Mini PC NUC8i7INH a NUC8i5INH
Intel® NUC 11 Performance kit – NUC11PAHi70Z, NUC11PAHi50Z, NUC11PAHi30Z, NUC11PAHi3, NUC11PAHi5, NUC11PAHi7, NUC11PAKi3, NUC11PAKi5, NUC11PAKi7
Intel® NUC 11 Performance Mini PC - NUC11PAQi50WA, NUC11PAQi70QA
Intel® NUC Kit - NUC5i3RYH, NUC5i7RYH, NUC5i5RYK, NUC5i5RYH, NUC5i3RYK, NUC5i5RYHS, NUC5i3RYHS, NUC5i3RYHSN.
Intel® NUC Kit - NUC8i7HNK, NUC8i7HVK
Intel® NUC 8 Enthusiast - NUC8i7HVKVA, NUC8i7HVKVAW
Intel® NUC 8 Business - NUC8i7HNKQC
Intel® NUC Kit - DE3815TYKHE
Intel® NUC Board - DE3815TYBE

Intel® NUC M15 Laptop Kit
Intel® NUC 10 Performance kit - NUC10i7FNHN, NUC10i5FNKN, NUC10i5FNHN, NUC10i7FNKN, NUC10i3FNHN, NUC10i3FNKN
Intel® NUC 10 Performance Mini PC - NUC10i5FNHJA, NUC10i3FNHF, NUC10i7FNKPA, NUC10i5FNHCA, NUC10i3FNHFA, NUC10i5FNHJ, NUC10i7FNHC, NUC10i7FNHJA, NUC10i3FNHJA, NUC10i3FNK, NUC10i7FNHAA, NUC10i5FNH, NUC10i5FNK, NUC10i7FNH, NUC10i5FNHF, NUC10i5FNKPA, NUC10i3FNH, NUC10i7FNK, NUC10i7FNKP, NUC10i5FNKP
Intel® NUC 8 Compute Element - CM8i7CB, CM8i3CB, CM8CCB, CM8i5CB, CM8PCB
Intel® NUC 8 Rugged Kit NUC8CCHKRN, NUC8CCHKR
Intel® NUC 8 Rugged Board - NUC8CCHBN
Intel® NUC Board - NUC5i3MYBE
Intel® NUC Kit - NUC5i3MYHE
Intel® NUC 11 Pro Kit - NUC11TNHi70Z, NUC11TNKi70Z, NUC11TNKi30Z, NUC11TNHi30Z, NUC11TNKi50Z, NUC11TNHi50Z, NUC11TNBi30Z, NUC11TNBi50Z, NUC11TNBi70Z, NUC11TNHi3, NUC11TNHi5

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Aktualizácia sa týka aj firmvéru serverov (BIOS upgrade).
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
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.
Manažmentové rozhrania zariadení a serverov odporúčame nesprístupňovať z verejného Internetu.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00740.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00720.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00716.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00715.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00713.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00711.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00710.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00708.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00699.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00695.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00691.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00689.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00688.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00687.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00680.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00676.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00673.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00659.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00642.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00610.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00558.html

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

Identifikátor

LiteSpeed a OpenLiteSpeed - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť LiteSpeed Technologies vydala bezpečnostné aktualizácie na produkty LiteSpeed a OpenLiteSpeed, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a v kombinácii s ostatnými umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.11.2022

CVE

CVE-2022-0072, CVE-2022-0073, CVE-2022-0074

Zasiahnuté systémy

OpenLiteSpeed vo verzii staršej ako v1.7.16.1
LiteSpeed vo verzii staršej ako 6.0.12

Následky

Eskalácia privilégií
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://unit42.paloaltonetworks.com/openlitespeed-vulnerabilities/
https://thehackernews.com/2022/11/multiple-high-severity-flaw-affect.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HPE produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v HPE ProLiant DL/ML zariadeniach s určitými Intel procesormi, spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a spôsobiť narušenie dôvernosti a integrity systému.

Dátum prvého zverejnenia varovania

08.11.2022

CVE

CVE-2021-33159, CVE-2021-33895, CVE-2022-21198, CVE-2022-26006, CVE-2022-26845, CVE-2022-27497, CVE-2022-29466, CVE-2022-29515, CVE-2022-29893

Zasiahnuté systémy
HPE StoreVirtual 3000 File Controller vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 1450 Storage vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 1550 Storage vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 1650 Storage vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 1850 Storage vo verzii staršej ako 3.04_08_04_2022
HPE StoreVirtual File Controller vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 3850 Gateway Storage vo verzii staršej ako 3.04_08_04_2022
HPE StoreEasy 1650 Expanded Storage vo verzii staršej ako 3.04_08_04_2022
HPE 3PAR StoreServ File Controller v3 System vo verzii staršej ako 3.04_08_04_2022
HPE StoreVirtual 3000 Storage vo verzii staršej ako 3.04_08_04_2022
HPE BackBox Software T0954 T0954V04^AAO, T0954V04^AAQ, T0954V04^AAR a T0954V04^AAS
HPE ProLiant XL740f Gen9 Server vo verzii staršej ako v3.04_08-04-2022
HPE ProLiant XL750f Gen9 Server vo verzii staršej ako v3.04_08-04-2022
HPE ProLiant XL730f Gen9 Server vo verzii staršej ako v3.04_08-04-2022
HPE ProLiant XL270d Gen9 Accelerator Tray 2U Configure-to-order Server vo verzii staršej ako v3.04_08-04-2022
HPE Synergy 480 Gen9 Compute Module vo verzii staršej ako v3.04_08-04-2022
HPE Synergy 660 Gen9 Compute Module vo verzii staršej ako v3.04_08-04-2022
HPE ProLiant m510 Server Cartridge vo verzii staršej ako 1.96_10-13-2022
HPE ProLiant BL460c Gen9 Server Blade vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant BL480c Server Blade vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant BL660c Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL60 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL80 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL160 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL180 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL120 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL360 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL380 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL560 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant ML110 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant ML150 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant ML350 Gen9 Server vo verzii staršej ako 3.04_08-04-2022 - Only CVE-2022-26006
HPE ProLiant DL20 Gen10 Plus server vo verzii staršej ako 1.64_10-20-2022 - Only CVE-2022-21198
HPE ProLiant MicroServer Gen10 Plus v2 vo verzii staršej ako 1.64_10-20-2022 - Only CVE-2022-21198
HPE ProLiant ML30 Gen10 Plus server vo verzii staršej ako 1.64_10-20-2022 - Only CVE-2022-21198
HPE ProLiant ML30 Gen10 Plus server vo verzii staršej ako SPS_E3_06.00.03.204.0, CSME 15.0.42
HPE ProLiant DL20 Gen10 Plus server vo verzii staršej ako SPS_E3_06.00.03.204.0, CSME 15.0.42
HPE ProLiant MicroServer Gen10 Plus v2 vo verzii staršej ako SPS_E3_06.00.03.204.0, CSME 15.0.42
HPE ProLiant DL20 Gen9 Server vo verzii staršej ako SPS_E3_04.01.04.700.0 CSME 11.8.93
HPE ProLiant ML30 Gen9 Server vo verzii staršej ako SPS_E3_04.01.04.700.0 CSME 11.8.93

Následky
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Aktualizácia sa týka aj firmvéru serverov (BIOS upgrade). 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. Manažmentové rozhrania zariadení a serverov odporúčame nesprístupňovať z verejného Internetu.

Zdroje
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04375en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04376en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04379en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04380en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04374en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04377en_us https://www.redpacketsecurity.com/intel-amt-privilege-escalation-cve-2022-26845/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch Cisco Adaptive Security Appliance (ASA) Software a Firepower Threat Defense (FTD), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.11.2022

CVE

CVE-2022-20713, CVE-2022-20745, CVE-2022-20826, CVE-2022-20831, CVE-2022-20832, CVE-2022-20833, CVE-2022-20854, CVE-2022-20918, CVE-2022-20922, CVE-2022-20924, CVE-2022-20925, CVE-2022-20926, CVE-2022-20927, CVE-2022-20928, CVE-2022-20932, CVE-2022-20934, CVE-2022-20938, CVE-2022-20940, CVE-2022-20941, CVE-2022-20943, CVE-2022-20946, CVE-2022-20947, CVE-2022-20949, CVE-2022-20950

Zasiahnuté systémy

Cisco Adaptive Security Appliance (ASA) Software
Cisco Firepower Threat Defense (FTD)
Cisco Snort 3 Detection Engine
Cisco Firepower Threat Defense Software SIP
Cisco Server Message Block Version 2
Cisco Firepower Management Center (FMC)
Simple Network Management Protocol
Cisco Next-Generation Intrusion Prevention System (NGIPS)
Cisco Secure Firewalls 3100 Series

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-bb-rCgtmY2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-mgmt-privesc-7GqR2th
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-fxos-cmd-inj-Q9bLNsrK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xxe-MzPC4bYd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-LATZYzxs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-info-disc-UghNRRhP
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-Z3B5MY35
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-vp-authz-N2GckjN6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssl-client-dos-cCrQPkA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fw3100-secure-boot-5M8mUh26
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-gre-dos-hmedHQPM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcsfr-snmp-access-6gqgtJ4S
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dos-OwEunWJN
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmp-dos-qsqBNM6x
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dap-dos-GhYZBxDU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-webvpn-LOeKsNmO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-smb-3nfhJtr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdsnort3sip-dos-A4cHeArC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

AMD produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť AMD vydala bezpečnostné aktualizácie na svoje portfólio grafických kariet AMD Radeon, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.11.2022

CVE

CVE-2020-12930, CVE-2020-12931, CVE-2021-26360, CVE-2021-26391, CVE-2021-26392, CVE-2021-26393

Zasiahnuté systémy

AMD Radeon RX 5000 Series
AMD Radeon PRO W5000 Series
AMD Radeon RX 6000 Series
AMD Radeon PRO W6000 Series
AMD Radeon™ RX Vega Series Graphics Cards vo všetkých verziách
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

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://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1029
https://www.redpacketsecurity.com/multiple-amd-graphics-products-code-execution-cve-2021-26360/

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

Identifikátor

Google Android - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj mobilný operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu obísť autentifikáciu, získať neoprávnený prístup do systému a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.11.2022

CVE

CVE-2021-1050, CVE-2021-35108, CVE-2021-35109, CVE-2021-35132, CVE-2021-35135, CVE-2021-39661, CVE-2022-20414, CVE-2022-20426, CVE-2022-20441, CVE-2022-20445, CVE-2022-20446, CVE-2022-20447, CVE-2022-20448, CVE-2022-20450, CVE-2022-20451, CVE-2022-20452, CVE-2022-20453, CVE-2022-20454, CVE-2022-20457, CVE-2022-20462, CVE-2022-20463, CVE-2022-20465, CVE-2022-2209, CVE-2022-25671, CVE-2022-25724, CVE-2022-25741, CVE-2022-25743, CVE-2022-2984, CVE-2022-2985, CVE-2022-32601, CVE-2022-32602, CVE-2022-33234, CVE-2022-33236, CVE-2022-33237, CVE-2022-33239, CVE-2022-38669, CVE-2022-38670, CVE-2022-38672, CVE-2022-38673, CVE-2022-38676, CVE-2022-38690, CVE-2022-39105

Zasiahnuté systémy

Google Android 10,11,12,12.1 a 13 na security patch úrovni staršej ako 2022-11-05

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://source.android.com/docs/security/bulletin/2022-11-01
https://www.sammobile.com/news/nasty-vulnerability-shows-galaxy-phones-can-be-safer-than-google-pixels/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Aiphone produkty - bezpečnostná zraniteľnosť

Popis

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zneužitia brute force metódy získať neoprávnený prístup do systému, eskalovať svoje privilégiá a následne vykonať neoprávnené zmeny v systéme.
Vzhľadom na to, že sa jedná o prístupové zariadenie na otváranie dverí, kompromitácia umožňuje neautorizovaný vstup do priestorov.
Na bezpečnostnú zraniteľnosť v produktoch vyrobených pred 7.12.2021 neexistuje záplata.

Dátum prvého zverejnenia varovania

07.11.2022

CVE

CVE-2022-40903

Zasiahnuté systémy

Aiphone GT-DMB-N vyrobené pred 7.12.2021
Aiphone GT-DMB-LVN vyrobené pred 7.12.2021
Aiphone GT-DB-VN vyrobené pred 7.12.2021

Následky

Neoprávnený prístup do systému
Eskalácia privilégií
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či nepoužívate predmetný zabezpečovací systém v zraniteľnej verzii. V prípade že áno, odporúčame rozšíriť zabezpečenie o dodatočné zabezpečovacie mechanizmy alebo prejsť na iný produkt bez známych bezpečnostných zraniteľností.

Zdroje

https://promon.co/security-news/aiphone-vulnerability/
https://www.cybersecurity-help.cz/vdb/SB2022111124
https://www.darkreading.com/iot/knock-knock-aiphone-bug-allows-cyberattackers-to-literally-open-physical-doors