NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

No: B20240220

BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 02. 2024 - 20. 02. 2024

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
Web: https://www.sk-cert.sk

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

Identifikátor

Schneider Electric produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-0568 sa nachádza v produktovej rade Harmony Control Relay, spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom NFC komunikácie vykonať neoprávnené zmeny v konfigurácii zasiahnutého systému a získať tak neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme, spôsobiť zneprístupnenie služby a eskalovať privilégiá.

Dátum prvého zverejnenia varovania

13.2.2024

CVE

CVE-2023-6408, CVE-2023-6409, CVE-2023-27975, CVE-2024-0568, CVE-2024-0865, CVE-2018-7855

Zasiahnuté systémy

Modicon M340 CPU
Modicon M580 CPU
Modicon M580 CPU Safety
EcoStruxure™ Control Expert
EcoStruxure™ Process Expert
Harmony Control Relay RMNF22TB30
Harmony Timer Relay RENF22R2MMW
EcoStruxure IT Gateway
Modicon M580
Modicon M340
Modicon Premium
Modicon Quantum

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.
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. Ak je potrebný vzdialený prístup,

použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-044-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-044-01.pdf
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-044-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-044-02.pdf
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2024-044-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2024-044-03.pdf
https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2019-134-11&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2019-134-11_Modicon_Controllers_Security_Notification.pdf

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

Identifikátor

IBM QRadar - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na produkty QRadar, QRadar SIEM a QRadar Wincollect, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2023-45133 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v produkte IBM QRadar a IBM QRadar Wincollect a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.2.2024

CVE

CVE-2023-44981, CVE-2023-45133, CVE-2023-38545, CVE-2023-4807, CVE-2023-45857, CVE-2023-43642, CVE-2023-3611, CVE-2023-3776, CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-37920

Zasiahnuté systémy

IBM QRadar Use Case Manager vo verzii staršej ako 3.9.0
QRadar SIEM vo verzii staršej ako 7.5 - 7.5.0 UP7 (vrátane)
QRadar WinCollect Agent vo verzii staršej ako 10.1.9

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.ibm.com/support/pages/node/7117881
https://www.ibm.com/support/pages/node/7117883
https://www.ibm.com/support/pages/node/7117884

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

Identifikátor

Linux Debian - viacero bezpečnostných zraniteľností

Popis

Vývojári distribúcie operačného systému Debian (Linux) vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2023-45235 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v komponente EDK2 a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v priľahlom sieťovom segmente, vykonaním škodlivého kódu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.2.2024

CVE

CVE-2022-36763, CVE-2022-36764, CVE-2022-36765, CVE-2023-45230, CVE-2023-45229, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2024-0985, CVE-2024-0985, CVE-2023-4408, CVE-2023-5517, CVE-2023-5679, CVE-2023-6516, CVE-2023-50387, CVE-2023-50868

Zasiahnuté systémy

Debian s komponentom edk2 vo verzii staršej ako 2020.11-2+deb11u2
Debian s komponentom postgresql-13 vo verzii staršej ako 13.14-0+deb11u1
Debian s komponentom postgresql-15 vo verzii staršej ako 15.6-0+deb12u1
Debian s komponentom bind9 vo verzii staršej ako 1:9.18.24-1

Následky

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

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://lists.debian.org/debian-security-announce/2024/msg00031.html
https://lists.debian.org/debian-security-announce/2024/msg00029.html
https://lists.debian.org/debian-security-announce/2024/msg00030.html
https://lists.debian.org/debian-security-announce/2024/msg00028.html

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

Identifikátor

Ubuntu - viacero bezpečnostných zraniteľnosti

Popis

Vývojári distribúcie Ubuntu operačného systému Linux vydali bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-23222 sa nachádza v komponente webkit2gtk, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky zrealizovať cross-site scripting útok, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme, vykonať škodlivý kód a spôsobiť zneprístupnenie služby. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

13.2.2024

CVE

CVE-2024-23222, CVE-2024-23213, CVE-2024-23206, CVE-2024-1141

Zasiahnuté systémy

Ubuntu 23.10 vo verziách balíkov starších ako
python3-glance-store - 4.6.1-0ubuntu1.1
libjavascriptcoregtk-4.0-18 - 2.42.5-0ubuntu0.23.10.2
libjavascriptcoregtk-4.1-0 - 2.42.5-0ubuntu0.23.10.2
libjavascriptcoregtk-6.0-1 - 2.42.5-0ubuntu0.23.10.2
libwebkit2gtk-4.0-37 - 2.42.5-0ubuntu0.23.10.2
libwebkit2gtk-4.1-0 - 2.42.5-0ubuntu0.23.10.2
libwebkitgtk-6.0-4 - 2.42.5-0ubuntu0.23.10.2

Ubuntu 22.04 vo verziách balíkov starších ako
python3-glance-store - 3.0.0-0ubuntu1.4
libjavascriptcoregtk-4.0-18 - 2.42.5-0ubuntu0.22.04.2
libjavascriptcoregtk-4.1-0 - 2.42.5-0ubuntu0.22.04.2
libjavascriptcoregtk-6.0-1 - 2.42.5-0ubuntu0.22.04.2
libwebkit2gtk-4.0-37 - 2.42.5-0ubuntu0.22.04.2
libwebkit2gtk-4.1-0 - 2.42.5-0ubuntu0.22.04.2
libwebkitgtk-6.0-4 - 2.42.5-0ubuntu0.22.04.2

Ubuntu 20.04 vo verziách balíkov starších ako
python3-glance-store - 2.0.0-0ubuntu4.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 alebo vzdialené vykonanie kódu, je dobrou praxou 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://ubuntu.com/security/notices/USN-6631-1 https://ubuntu.com/security/notices/USN-6630-1

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 s označením CVE-2023-39425 sa nachádza v produkte Intel Driver & Support Assistant, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.2.2024

CVE

CVE-2023-39425, CVE-2023-34351 , CVE-2023-33875, CVE-2023-39941, CVE-2023-22293, CVE-2022-43702, CVE-2022-43701, CVE-2022-43703

Zasiahnuté systémy

Arm DS for Intel® SoC FPGA
Intel DSA
Intel PCM
Intel PROSet/Wireless Wi-Fi
Intel Killer Wi-Fi
Intel SUR software
Intel Thunderbolt DCH driver
Intel® JHL8440 Thunderbolt™ 4
Intel® Optimization for TensorFlow
ACAT software
Intel® OpenBMC
Intel® One Boot Flash
Intel® Chipset Driver Software
Intel® Optane™ PMem 100 Series
Intel® Optane™ PMem 200 Series
Intel® Optane™ PMem 300 Series
Intel® Virtual RAID on CPU (VROC)
Intel® Extreme Tuning Utility (XTU)
Intel® oneAPI Toolkit
Intel® Performance Maximizer (PM)
Intel® CIP
Intel® Memory and Storage Tool (MAS)
Intel® Driver & Support Assistant (DSA)
Intel® Binary Configuration Tool
Intel® QSFP+ Configuration Utility
Intel Unite® Client
Intel® Battery Life Diagnostic Tool
Intel® SDK for OpenCL™
Intel® Ethernet tools and driver
Intel® Implicit SPMD Program Compiler (ISPC)
Intel® System Usage Report (SUR)

Intel® QuickAssist Technology (QAT)
Intel® Server Platform Services (SPS)
Intel® System Usage Report (SUR)
Intel® MPI Library
Intel® Unison™
Intel® System Support Utility (SSU)
Intel® Software Guard Extensions (SGX) Data Center Attestation Primitives (DCAP)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Eskalácia privilégií
Zneprístupnenie služby
Neoprávnená zmena v systéme
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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00851.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00895.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00903.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00913.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00922.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00927.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00928.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00930.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00947.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00948.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00953.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00954.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00955.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00956.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00958.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00959.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00967.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00969.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00973.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00974.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00981.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00987.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00988.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00992.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00993.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00994.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00998.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01000.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01003.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01004.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01005.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01006.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01011.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01014.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
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 s označením CVE-2023-23583 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v produkte SimpliVity 380 Gen10 Plus a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa, prostredníctvom zneužitia out-of-bounds zápisu, eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti môžu zneužiť out-of-bounds zápis a spôsobiť vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

12.2.2024

CVE

CVE-2023-20577, CVE-2023-20587, CVE-2023-23583, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2023-31346, CVE-2023-31347, CVE-2023-48795

Zasiahnuté systémy

HPE SimpliVity 380 Gen10 Plus s HPE OmniStack Firmware vo verzii staršej ako 2024_0131
HPE ProLiant DL325 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DL345 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DL365 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DL385 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DX365 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DX385 Gen11 Server vo verzii staršej ako v1.58_01_04_2024
HPE ProLiant DL385 Gen10 Server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL325 Gen10 Server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL385 Gen10 Plus server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL325 Gen10 Plus server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL365 Gen10 Plus server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DX385 Gen10 Plus server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL385 Gen10 Plus v2 server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL345 Gen10 Plus server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DL325 Gen10 Plus v2 server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DX325 Gen10 Plus v2 server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant DX385 Gen10 Plus v2 server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant XL225n Gen10 Plus 1U Node vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant XL645d Gen10 Plus Server vo verzii staršej ako v3.00_01_26_2024
HPE ProLiant XL675d Gen10 Plus Server vo verzii staršej ako v3.00_01_26_2024

Následky

Eskalácia privilégií
Zneprístupnenie služby

Neoprávnený prístup k citlivým údajom
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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04591en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04594en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04566en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04592en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04596en_us

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

Identifikátor

SUSE Linux Kernel - viacero bezpečnostných zraniteľností

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-1086 nachádzajúca sa v komponente nf_tables spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom znovupoužitia uvoľnenej pamäte eskalovať svoje privilégiá na zasiahnutom systéme.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme, spôsobiť zneprístupnenie služby a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

15.2.2024

CVE

CVE-2024-1086, CVE-2024-0775, CVE-2024-0565, CVE-2023-51782, CVE-2023-51780, CVE-2023-51043, CVE-2023-47233, CVE-2023-46838, CVE-2023-6915, CVE-2023-6536, CVE-2023-6535, CVE-2023-6356, CVE-2023-6040, CVE-2021-33631

Zasiahnuté systémy

SUSE Linux Enterprise Micro 5.1, 5.2 a Rancher 5.2 bez aplikovanej bezpečnostnej záplaty

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

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 získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, 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.suse.com/support/update/announcement/2024/suse-su-20240463-1/

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

Identifikátor

Eset produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť ESET vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť. Zero-Day bezpečnostná zraniteľnosť s označením CVE-2024-0353 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom odstránenia vybraných súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.2.2024

CVE

CVE-2024-0353

Zasiahnuté systémy

ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium a ESET Security Ultimate vo verzii staršej ako 17.0.10.0
ESET Endpoint Antivirus for Windows a ESET Endpoint Security for Windows vo verzii staršej ako 11.0.2032.0, 10.1.2063.0, 10.0.2052.0, 9.1.2071.0 a 8.1.2062.0
ESET Server Security for Windows Server vo verzii staršej ako 10.0.12015.0, 9.0.12019.0, 8.0.12016.0 a 7.3.12013.0
ESET Mail Security for Microsoft Exchange Server vo verzii staršej ako 10.1.10014.0, 10.0.10018.0, 9.0.10012.0, 8.0.10024.0 a 7.3.10018.0
ESET Mail Security for IBM Domino vo verzii staršej ako 10.0.14007.0, 9.0.14008.0, 8.0.14014.0 a 7.3.14006.0
ESET Security for Microsoft SharePoint vo verzii staršej ako Server 10.0.15005.0, 9.0.15006.0, 8.0.15012.0 a 7.3.15006.0
ESET File Security for Microsoft Azure s ESET Server Security for Windows Server vo verzii staršej ako 10.0.12015.0, 9.0.12019.0, 8.0.12016.0 a 7.3.12013.0

Následky

Eskalácia privilégií
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://support.eset.com/en/ca8612-eset-customer-advisory-link-following-local-privilege-escalation-vulnerability-in-eset-products-for-windows-fixed

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

Identifikátor

F5 produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s označeniami CVE-2024-23982 a CVE-2024-21789 sa nachádzajú v produktoch BIG-IP Policy Enforcement Manager (PEM) a BIG-IP (Advanced WAF/ASM), spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnený prístup k citlivým údajom a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.2.2024

CVE

CVE-2023-5680, CVE-2024-23982, CVE-2024-21789, CVE-2024-23607

Zasiahnuté systémy

BIG-IP (PEM) vo verziách 17.1.0, 17.1.1, vo verziách od 16.1.0 do 16.1.4 (vrátane), vo verziách od 15.1.0 do 15.1.10 (vrátane)
BIG-IP (Advanced WAF/ASM) vo verzii staršej ako 17.1.1
F5OS-A vo verzii staršej ako 1.4.0
F5OS-C vo verzii staršej ako 1.6.0
BIND9 vo verziách od 9.11.3-S1 do 9.11.37-S1, vo verziách od 9.16.8-S1 do 9.16.45-S1 a vo verziách od 9.18.11-S1 do 9.18.21-S1

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

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.
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://my.f5.com/manage/s/article/K000135946
https://my.f5.com/manage/s/article/K000137270
https://my.f5.com/manage/s/article/K000132800
https://my.f5.com/manage/s/article/K000138618