BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 08. 2023 - 22. 08. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	RARLAB WinRAR - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	PDF XChange Editor - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Zyxel NBG6604 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Schneider Electric PowerLogic ION series - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	Red Lion mbNET/mbNET.rokey, Helmholz REX 200/REX 250 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	Jenkins pluginy - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
08.	ESET Smart Security - bezpečnostná zraniteľnosť	Vysoká	**7.8**
09.	HPE Produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Cisco Produkty - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
11.	OpenNMS Meridian and Horizon - bezpečnostná zraniteľnosť	Vysoká	**7.6**
12.	Rockwell Automation Armor PowerFlex - bezpečnostná zraniteľnosť	Vysoká	**7.5**
13.	Walchem Intuition 9 - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
14.	Atlassian Confluence - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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-1288

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

Identifikátor

RARLAB WinRAR - bezpečnostná zraniteľnosť

Popis

Spoločnosť RARLAB vydala bezpečnostnú aktualizáciu na svoj produkt WinRAR, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.08.2023

CVE

CVE-2023-40477

Zasiahnuté systémy

WinRAR vo verzii staršej ako 6.23

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa
https://www.zerodayinitiative.com/advisories/ZDI-23-1152/

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

Identifikátor

PDF XChange Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť PDF-XChange vydala bezpečnostnú aktualizáciu na svoj produkt PDF XChange Editor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.08.2023

CVE

CVE-2023-39483, CVE-2023-39484, CVE-2023-39485, CVE-2023-39486, CVE-2023-39487, CVE-2023-39488, CVE-2023-39489, CVE-2023-39490, CVE-2023-39491, CVE-2023-39492, CVE-2023-39493, CVE-2023-39494, CVE-2023-39495, CVE-2023-39496, CVE-2023-39497, CVE-2023-39498, CVE-2023-39499, CVE-2023-39500, CVE-2023-39501, CVE-2023-39502, CVE-2023-39503, CVE-2023-39504, CVE-2023-39505, CVE-2023-39506, CVE-2023-40468, CVE-2023-40469, CVE-2023-40470, CVE-2023-40471, CVE-2023-40472, CVE-2023-40473

Zasiahnuté systémy

PDF-XChange Editor vo verzii staršej ako V9 (9.5.368) a V10 (10.0.1)

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://www.zerodayinitiative.com/advisories/ZDI-23-1122/
https://www.zerodayinitiative.com/advisories/ZDI-23-1123/
https://www.zerodayinitiative.com/advisories/ZDI-23-1124/
https://www.zerodayinitiative.com/advisories/ZDI-23-1125/
https://www.zerodayinitiative.com/advisories/ZDI-23-1126/
https://www.zerodayinitiative.com/advisories/ZDI-23-1127/
https://www.zerodayinitiative.com/advisories/ZDI-23-1128/
https://www.zerodayinitiative.com/advisories/ZDI-23-1129/
https://www.zerodayinitiative.com/advisories/ZDI-23-1130/
https://www.zerodayinitiative.com/advisories/ZDI-23-1131/
https://www.zerodayinitiative.com/advisories/ZDI-23-1132/
https://www.zerodayinitiative.com/advisories/ZDI-23-1133/
https://www.zerodayinitiative.com/advisories/ZDI-23-1134/
https://www.zerodayinitiative.com/advisories/ZDI-23-1135/
https://www.zerodayinitiative.com/advisories/ZDI-23-1136/
https://www.zerodayinitiative.com/advisories/ZDI-23-1137/
https://www.zerodayinitiative.com/advisories/ZDI-23-1138/
https://www.zerodayinitiative.com/advisories/ZDI-23-1139/
https://www.zerodayinitiative.com/advisories/ZDI-23-1140/
https://www.zerodayinitiative.com/advisories/ZDI-23-1141/
https://www.zerodayinitiative.com/advisories/ZDI-23-1142/
https://www.zerodayinitiative.com/advisories/ZDI-23-1143/
https://www.zerodayinitiative.com/advisories/ZDI-23-1144/
https://www.zerodayinitiative.com/advisories/ZDI-23-1145/
https://www.zerodayinitiative.com/advisories/ZDI-23-1146/
https://www.zerodayinitiative.com/advisories/ZDI-23-1147/
https://www.zerodayinitiative.com/advisories/ZDI-23-1148/
https://www.zerodayinitiative.com/advisories/ZDI-23-1149/
https://www.zerodayinitiative.com/advisories/ZDI-23-1150/
https://www.zerodayinitiative.com/advisories/ZDI-23-1151/

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.08.2023

CVE

CVE-2023-2312, CVE-2023-4349, CVE-2023-4350, CVE-2023-4351, CVE-2023-4352, CVE-2023-4353, CVE-2023-4354, CVE-2023-4355, CVE-2023-4356, CVE-2023-4357, CVE-2023-4358, CVE-2023-4359, CVE-2023-4360, CVE-2023-4361, CVE-2023-4362, CVE-2023-4363, CVE-2023-4364, CVE-2023-4365, CVE-2023-4366, CVE-2023-4367, CVE-2023-4368

Zasiahnuté systémy

Chrome pre Mac vo verzii staršej ako 116.0.5845.96
Chrome pre Linux vo verzii staršej ako 116.0.5845.96/.97

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html

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

Identifikátor

Zyxel NBG6604 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Zyxel vydala bezpečnostnú aktualizáciu na svoj WiFi router NBG6604, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.08.2023

CVE

CVE-2023-33013

Zasiahnuté systémy

Zyxel NBG6604 vo verzii staršej ako 1.01(ABIR.2)C0

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.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-in-ntp-feature-of-nbg6604-home-router
https://exchange.xforce.ibmcloud.com/vulnerabilities/263522

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

Identifikátor

Schneider Electric PowerLogic ION series - bezpečnostná zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt PowerLogic ION series, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.08.2023

CVE

CVE-2022-46680

Zasiahnuté systémy

PowerLogic ION9000 vo verzii staršej ako 4.0.0
PowerLogic ION7400 vo verzii staršej ako 4.0.0
PowerLogic PM8000 vo verzii staršej ako 4.0.0
PowerLogic ION8650 vo všetkých verziách
PowerLogic ION8800 vo všetkých verziách
Legacy ION produkty vo všetkých verziách

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.
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://www.cisa.gov/news-events/ics-advisories/icsa-23-229-03

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

Identifikátor

Red Lion mbNET/mbNET.rokey, Helmholz REX 200/REX 250 - bezpečnostná zraniteľnosť

Popis

Spoločnosti Red Lion a Helmholz vydali bezpečnostné aktualizácie na svoje routre, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

17.08.2023

CVE

CVE-2023-34412

Zasiahnuté systémy

mbNET vo verzii firmvéru staršej ako 7.3.2
mbNET.rokey vo verzii firmvéru staršej ako 7.3.2
REX 200 vo verzii firmvéru staršej ako 7.3.2
REX 250 vo verzii firmvéru staršej ako 7.3.2

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://cert.vde.com/en/advisories/VDE-2023-029/
https://cert.vde.com/en/advisories/VDE-2023-012/

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

Identifikátor

Jenkins pluginy - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach pluginov pre open-source Java server Jenkins.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v plugine Cloudbees-folder, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.08.2023

CVE

CVE-2023-40336, CVE-2023-40337, CVE-2023-40338, CVE-2023-40339, CVE-2023-40340, CVE-2023-40341, CVE-2023-40342, CVE-2023-40343, CVE-2023-40344, CVE-2023-40345, CVE-2023-40346, CVE-2023-40347, CVE-2023-40348, CVE-2023-40349, CVE-2023-40350, CVE-2023-40351, CVE-2023-4301, CVE-2023-4302, CVE-2023-4303

Zasiahnuté systémy

Folders Plugin vo verzii staršej ako 6.848.ve3b_fd7839a_81
Blue Ocean Plugin vo verzii staršej ako 1.27.5.1
Config File Provider Plugin vo verzii staršej ako 953.v0432a_802e4d2
Delphix Plugin vo verzii staršej ako 3.0.3
Flaky Test Handler Plugin vo verzii staršej ako 1.2.3
Folders Plugin vo verzii staršej ako 6.848.ve3b_fd7839a_81
Fortify Plugin vo verzii staršej ako 22.2.39
NodeJS Plugin vo verzii staršej ako 1.6.0.1
Shortcut Job Plugin vo verzii staršej ako 0.5
Tuleap Authentication Plugin vo verzii staršej ako 1.1.21
Docker Swarm Plugin vo verzii staršej ako 1.11 (vrátane)
Favorite View Plugin vo verzii staršej ako 5.v77a_37f62782d (vrátane)
Gogs Plugin vo verzii staršej ako 1.0.15 (vrátane)
Maven Artifact ChoiceListProvider (Nexus) Plugin vo verzii staršej ako 1.14 (vrátane)

Následky

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

Odporúčania
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností. Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje
https://www.jenkins.io/security/advisory/2023-08-16/ https://www.securityweek.com/jenkins-patches-high-severity-vulnerabilities-in-multiple-plugins/

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

Identifikátor

ESET Smart Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť ESET vydala bezpečnostnú aktualizáciu na svoj produkt Smart Security, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.08.2023

CVE

CVE-2023-3160

Zasiahnuté systémy

ESET Smart Security s HIPS support modulom vo verzii staršej ako 1463

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://support.eset.com/en/ca8466-eset-customer-advisory-local-privilege-escalation-vulnerability-fixed-in-eset-security-products-for-windows
https://www.zerodayinitiative.com/advisories/ZDI-23-1114/

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

Identifikátor

HPE Produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť HPE vydala bezpečnostnú aktualizáciu na svoje produkty SimpliVity a Aruba Networking VIA, ktoré opravujú viacero bezpečnostných zraniteľností.
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

15.08.2023

CVE

CVE-2022-33894, CVE-2022-38087, CVE-2023-38401, CVE-2023-38402

Zasiahnuté systémy

HPE SimpliVity 380 Gen10 vo verzii OmniStack firmvéru staršej ako 2023_0803
HPE SimpliVity 380 Gen10 G vo verzii OmniStack firmvéru staršej ako 2023_0803
HPE SimpliVity 380 Gen10 H vo verzii OmniStack firmvéru staršej ako 2023_0803
HPE SimpliVity 190r Gen10 Server vo verzii OmniStack firmvéru staršej ako 2023_0803
HPE SimpliVity 170r Gen10 Server vo verzii OmniStack firmvéru staršej ako 2023_0803
HPE Aruba Networking Virtual Intranet Access (VIA) pre Microsoft Windows vo verzii staršej ako 4.6.0

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04463en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04527en_us

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

Identifikátor

Cisco Produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty ThousandEyes Enterprise Agent, 5000 Series ENCS, UCS C-Series M5 Rack Server a UCS E-Series M3 Server, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa 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

17.08.2023

CVE

CVE-2023-20217, CVE-2023-20224, CVE-2023-20228

Zasiahnuté systémy

Cisco ThousandEyes Enterprise Agent vo verzii staršej ako 0.230
Cisco 5000 Series ENCS vo verzii staršej ako 3.2.15.1 (Nov 2023)
Cisco UCS C-Series M5 Rack Server vo verzii staršej ako 4.3.2.230207
Cisco UCS E-Series M3 Server vo verzii staršej ako 3.2.15.1 (Nov 2023)

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thoueye-privesc-NVhHGwb3
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-va-priv-esc-PUdgrx8E
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-UMYtYEtr

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

Identifikátor

OpenNMS Meridian and Horizon - bezpečnostná zraniteľnosť

Popis

Spoločnosť OpenNMS vydala bezpečnostné aktualizácie na svoje produkty Meridian a Horizon, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvoreného XML dokumentu získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

12.08.2023

CVE

CVE-2023-0871

Zasiahnuté systémy

Meridian vo verzii staršej ako 2023.1.6, 2022.1.19, 2021.1.30, 2020.1.38
Horizon vo verzii staršej ako 32.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.
Výrobca odporúča zasiahnuté systémy neponechávať otvorené do verejného internetu.

Zdroje

https://opennms.atlassian.net/browse/NMS-16069?jql=text%20~%20%22CVE-2023-0871%22
https://nvd.nist.gov/vuln/detail/CVE-2023-0871

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

Identifikátor

Rockwell Automation Armor PowerFlex - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt PowerFlex, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania veľkého množstva sieťových príkazov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.08.2023

CVE

CVE-2023-2423

Zasiahnuté systémy

Armor PowerFlex vo verzii staršej ako v2.001

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://www.cisa.gov/news-events/ics-advisories/icsa-23-227-02

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

Identifikátor

Walchem Intuition 9 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Walchem vydala bezpečnostnú aktualizáciu firmvéru na svoj produkt Intuition 9, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

17.08.2023

CVE

CVE-2023-32202, CVE-2023-38422

Zasiahnuté systémy

Intuition 9 vo verzii firmvéru staršej ako v4.21

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.
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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-229-04

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

Identifikátor

Atlassian Confluence - bezpečnostná zraniteľnosť

Popis

Spoločnosť Atlassian vydala bezpečnostnú aktualizáciu na svoj produkt Confluence Server and Data Center, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.08.2023

CVE

CVE-2023-28709

Zasiahnuté systémy

Confluence Server and Data Center vo verzii staršej ako 7.13.19, 7.19.11, 8.4.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://jira.atlassian.com/browse/CONFSERVER-90185
https://confluence.atlassian.com/security/security-bulletin-august-15-2023-1276870882.html