



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - zero-day bezpečnostná zraniteľnosť	Vysoká	8.8
02.	VLC player - dve bezpečnostné zraniteľnosti	Vysoká	8.8
03.	Apache Tapestry - bezpečnostná zraniteľnosť	Vysoká	8.8
04.	Node.js snyk - bezpečnostná zraniteľnosť	Vysoká	8.8
05.	Avast a AVG Antivirus - bezpečnostná zraniteľnosť	Vysoká	8.8
06.	Rockwell Automation controllers - bezpečnostná zraniteľnosť	Vysoká	8.6
07.	snap-confine - bezpečnostná zraniteľnosť	Vysoká	8.4
08.	MS Edge - bezpečnostná zraniteľnosť	Vysoká	8.3
09.	Cisco IP Phone - bezpečnostná zraniteľnosť	Vysoká	8.1
10.	PowerISO - bezpečnostná zraniteľnosť	Vysoká	7.8
11.	Trend Micro Apex One - dve bezpečnostné zraniteľnosti	Vysoká	7.8
12.	AVEVA InTouch Access Anywhere - bezpečnostná zraniteľnosť	Vysoká	7.5
13.	Advantech iView - bezpečnostná zraniteľnosť	Vysoká	7.5
14.	VMware ESXi and vCenter Server - viacero bezpečnostných zraniteľností	Vysoká	7.5
15.	FreeBSD OS - bezpečnostná zraniteľnosť	Vysoká	7.3



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Google Chrome - zero-day bezpečnostná zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje zero-day bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2022

CVE

CVE-2022-4262

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 108.0.5359.94

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/2022/12/stable-channel-update-for-desktop.html>

<https://nvd.nist.gov/vuln/detail/CVE-2022-4262>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

VLC player - dve bezpečnostné zraniteľnosti

Popis

Vývojári aplikácie VLC vydali bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného mp4 súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.12.2022

CVE

CVE-2022-31693, CVE-2022-41325

Zasiiahnuté systémy

VLC media player vo verzii staršej ako 3.0.18

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

<http://www.videolan.org/security/sb-vlc3018.html>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Apache Tapestry - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Apache Tapestry zverejnili informácie o zraniteľnosti svojho produktu. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2022

CVE

CVE-2022-46366

Zasiiahnuté systémy

Apache Tapestry vo všetkých verziách

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, plugíny, SDK alebo moduly v zraniteľnej verzii. Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.

Zdroje

<https://www.redpacketsecurity.com/apache-tapestry-code-execution-cve-2022-46366/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Node.js snyk - bezpečnostná zraniteľnosť

Popis

Vývojári modulu Node.js vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.12.2022

CVE

CVE-2022-24441

Zasiahnuté systémy

Node.js snyk vo verzii staršej ako 1.1064.0

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.

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.redpacketsecurity.com/node-js-snyk-module-code-execution-cve-2022-24441/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Avast a AVG Antivirus - bezpečnostná zraniteľnosť

Popis

Vývojári programov Avast a AVG Antivirus vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia bližšie neurčenej zraniteľnosti v nástroji na odstraňovanie malvéru eskalovať svoje privilégia a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepriístupnenie služby.

Dátum prvého zverejnenia varovania

07.12.2022

CVE

CVE-2022-4173

Zasiahnuté systémy

Avast vo verzii staršej ako 22.10

AVG Antivirus vo verzii staršej ako 22.10

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://nvd.nist.gov/vuln/detail/CVE-2022-4173>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.6
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Rockwell Automation controllers - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoje portfólio riadiacich systémov, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorených Ethernetových rámcov spôsobiť znepřístupnenie služby.

Dátum prvého zverejnenia varovania

08.12.2022

CVE

CVE-2022-3752

Zasiiahnuté systémy

CompactLogix 5380 vo verzii firmvéru staršej ako 32.016

Compact GuardLogix 5380 vo verzii firmvéru staršej ako 32.016

CompactLogix 5480 vo verzii firmvéru staršej ako 32.016

ControlLogix 5580 vo verzii firmvéru staršej ako 32.016

GuardLogix 5580 vo verzii firmvéru staršej ako 32.016

Pre firmvér vo verzii 33 je mitigácia prítomná v update 33.015, alternatívne 34.011

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiiahnutých 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/uscert/ics/advisories/icsa-22-342-03>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.4
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

snap-confine - bezpečnostná zraniteľnosť

Popis

Spoločnosť Canonical vydala bezpečnostnú aktualizáciu na svoj produkt snapd, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.12.2022

CVE

CVE-2022-3328

Zasiahnuté systémy

snapd vo verzii staršej ako 2.57.6-1

Ubuntu 16.04 vo verzii staršej ako 2.54.3+16.04.0ubuntu0.1~esm5

Ubuntu 18.04 vo verzii staršej ako 2.57.5+18.04ubuntu0.1

Ubuntu 20.04 vo verzii staršej ako 2.57.5+20.04ubuntu0.1

Ubuntu 22.04 vo verzii staršej ako 2.57.5+22.04ubuntu0.1

Ubuntu 22.10 vo verzii staršej ako 2.57.5+22.10ubuntu0.1

Ubuntu 14.04 LTS vo všetkých verziách, end of life

Upstream zatiaľ bez záplaty

Následky

Eskalácia privilégií na používateľa root

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.qualys.com/2022/11/30/cve-2022-3328/advisory-snap.txt><https://security.snyk.io/vuln/SNYK-DEBIAN12-SNAPD-3151088><https://www.securityweek.com/three-innocuous-linux-vulnerabilities-chained-obtain-full-root-privileges>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.3
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

MS Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Edge, ktorá opravuje bezpečnostnú zraniteľnosť.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.12.2022

CVE

CVE-2022-44708

Zasiahnuté systémy

Microsoft Edge pre iOS vo verzii staršej ako 108.0.1462.41

Microsoft Edge (Chromium-based) vo verzii staršej ako 108.0.1462.41

Následky

Eskalácia privilégií

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708>

<https://www.redpacketsecurity.com/microsoft-edge-chromium-based-privilege-escalation-cve-2022-44708/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.1
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Cisco IP Phone - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov IP Phone 7800 a 8800. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom metódy stack overflow vykonať neoprávnené zmeny v systéme a znepřístupnenie služby.

Dátum prvého zverejnenia varovania

08.12.2022

CVE

CVE-2022-20968

Zasiahnuté systémy

Cisco IP Phone Firmware vo verzii staršej ako 14.2 (vrátane)

Následky

Neoprávnená zmena v systéme
Znepřístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Pre dočasnú mitigáciu výrobca odporúča vypnúť Cisco Discovery Protocol.

Zdroje

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

PowerISO - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu PowerISO. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.12.2022

CVE

CVE-2022-41992

Zasiahnuté systémy

PowerISO vo verzii staršej ako 8.3 (vrátane)

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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 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://talosintelligence.com/vulnerability_reports/TALOS-2022-1644



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Trend Micro Apex One - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoje portfólio produktov Apex One, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégia a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

01.12.2022

CVE

CVE-2022-45797, CVE-2022-45798

Zasiahnuté systémy

Apex One vo verzii staršej ako SP1 CP b11136

Apex One as a Service vo verzii staršej ako Hotfix Build 202211 Agent 14.0.11840

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://success.trendmicro.com/dcx/s/solution/000291830?language=en_US



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

AVEVA InTouch Access Anywhere - bezpečnostná zraniteľnosť

Popis

Spoločnosť AVEVA vydala bezpečnostnú aktualizáciu na svoj produkt InTouch Access Anywhere, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

08.12.2022

CVE

CVE-2022-23854

Zasiahnuté systémy

InTouch Access Anywhere Secure Gateway 2020 R2 vo verzii staršej ako 20.1.0 Hotfix

InTouch Access Anywhere Secure Gateway 2020b vo verzii staršej ako 20.0.1 Hotfix

Následky

Neoprávnený prístup k citlivým údajom

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 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.cisa.gov/uscert/ics/advisories/icsa-22-342-02>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Advantech iView - bezpečnostná zraniteľnosť

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt iView, 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.

Dátum prvého zverejnenia varovania

08.12.2022

CVE

CVE-2022-3323

Zasiahnuté systémy

iView vo verzii staršej ako v5.7.04.6583.

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 infraštruktúry.

Zdroje

<https://www.cisa.gov/uscert/ics/advisories/icsa-22-342-01>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

VMware ESXi and vCenter Server - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom narušenia pamäte spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.12.2022

CVE

CVE-2022-31696, CVE-2022-31697, CVE-2022-31698, CVE-2022-31699

Zasiiahnuté systémy

VMware vCenter Server 7.0 vo verzii staršej ako U3i
vCenter Server 6.7 vo verzii staršej ako U3s
vCenter Server 6.5 vo verzii staršej ako U3u
VMware ESXi 7.0 vo verzii staršej ako ESXi70U3si-20841705
VMware ESXi 6.7 vo verzii staršej ako ESXi670-202210101-SG
VMware ESXi 6.5 vo verzii staršej ako ESXi650-202210101-SG

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://www.vmware.com/security/advisories/VMSA-2022-0030.html>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.3
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

FreeBSD OS - bezpečnostná zraniteľnosť

Popis

Vývojári operačného systému FreeBSD vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom čiastočného (keďže ping process operuje len v rámci sandboxu) narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.11.2022

CVE

CVE-2022-23093

Zasiahnuté systémy

Free BSD vo verzii staršej ako 13.1-STABLE
Free BSD vo verzii staršej ako 13.1-RELEASE-p5
Free BSD vo verzii staršej ako 12.4-STABLE
Free BSD vo verzii staršej ako 12.4-RC2-p2
Free BSD vo verzii staršej ako 12.3-RELEASE-p10

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nie sú založené na predmetnom operačnom systéme v zraniteľnej verzii (ako napr. firewall OPNsense). V prípade, že áno, zabezpečte aktualizáciu softvéru ako aj komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

Odporúčame tiež zvážiť konfiguráciu automatických aktualizácií podľa návodu na <https://docs.freebsd.org/en/books/handbook/cutting-edge/> .

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.freebsd.org/security/advisories/FreeBSD-SA-22:15.ping.asc>
<https://thehackernews.com/2022/12/critical-ping-vulnerability-allows.html>
<https://vuldb.com/?id.214613>
<https://nakedsecurity.sophos.com/2022/12/05/ping-of-death-freebsd-fixes-crashtastic-bug-in-network-tool/>