



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	8.8
02.	tenable.io, tenable.sc a Nessus - bezpečnostná zraniteľnosť	Vysoká	8.8
03.	OpenSSH Server - kritická bezpečnostná zraniteľnosť	Vysoká	8.1
04.	Horner Automation Cscape Envision RV - tri bezpečnostné zraniteľnosti	Vysoká	7.8
05.	Johnson Controls System Configuration Tool - dve bezpečnostné zraniteľnosti	Vysoká	7.5
06.	HP Factory Preinstalled Images - 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 - 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 vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.02.2023

CVE

CVE-2023-0696, CVE-2023-0697, CVE-2023-0698, CVE-2023-0699, CVE-2023-0700, CVE-2023-0701, CVE-2023-0702, CVE-2023-0703, CVE-2023-0704, CVE-2023-0705

Zasiahnuté systémy

Chrome vo verzii staršej ako 110.0.5481.77/.78 pre Windows

Chrome vo verzii staršej ako 110.0.5481.77 pre Mac a Linux

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/2023/02/stable-channel-update-for-desktop.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

tenable.io, tenable.sc a Nessus - bezpečnostná zraniteľnosť

Popis

Spoločnosť Tenable vydala bezpečnostnú aktualizáciu na produkty tenable.io, tenable.sc a Nessus, ktoré opravujú bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégia a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.01.2023

CVE

CVE-2023-0524

Zasiahnuté systémy

tenable.io, tenable.sc a Nessus s pluginmi so sériovým číslom nižším ako #202212212055

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://www.tenable.com/security/tns-2023-04><https://nvd.nist.gov/vuln/detail/CVE-2023-0524>



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

OpenSSH Server - kritická bezpečnostná zraniteľnosť

Popis

Vývojári nástroja OpenSSH Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

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

Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

08.02.2023

CVE

CVE-2023-25136

Zasiahnuté systémy

OpenSSH vo verzii staršej ako 9.2p1

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.openssh.com/txt/release-9.2>

<https://jfrog.com/blog/openssh-pre-auth-double-free-cve-2023-25136-writeup-and-proof-of-concept/>

https://bugzilla.mindrot.org/show_bug.cgi?id=3522

<https://blog.qualys.com/vulnerabilities-threat-research/2023/02/03/cve-2023-25136-pre-auth-double-free-vulnerability-in-openssh-server-9-1>

<https://thehackernews.com/2023/02/openssh-releases-patch-for-new-pre-auth.html>



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

Horner Automation Cscape Envision RV - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj softvér pre manažment vzdialeného prístupu do riadiacich zariadení Cscape Envision RV, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.02.2023

CVE

CVE-2023-0621, CVE-2023-0622, CVE-2023-0623

Zasiahnuté systémy

Cscape Envision RV vo verzii staršej ako 4.70

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

<https://www.cisa.gov/uscert/ics/advisories/icsa-23-040-04>



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

Johnson Controls System Configuration Tool - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Johnson Controls vydala bezpečnostnú aktualizáciu na svoj produkt System Configuration Tool, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

09.02.2023

CVE

CVE-2022-21939, CVE-2022-21940

Zasiiahnuté systémy

SCT 14 vo verzii staršej ako 14.2.3

SCT 15 vo verzii staršej ako 15.0.3

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.cisa.gov/uscert/ics/advisories/icsa-23-040-03>



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

HP Factory Preinstalled Images - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hewlett Packard zverejnila informácie o zraniteľnosti produktu Factory Preinstalled Images. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov eskalovať svoje privilégia a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

02.02.2023

CVE

CVE-2022-38396

Zasiahnuté systémy

HP Factory Preinstalled Images nainštalované na Windows 10 vo verzii staršej ako 21H2

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.

Zdrojehttps://support.hp.com/ie-en/document/ish_7620368-7620413-16<https://exchange.xforce.ibmcloud.com/vulnerabilities/246538>