BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 09. 2022 - 04. 10. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Google 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

27.09.2022

CVE

CVE-2022-3201, CVE-2022-3304, CVE-2022-3305, CVE-2022-3306, CVE-2022-3307, CVE-2022-3308, CVE-2022-3309, CVE-2022-3310, CVE-2022-3311, CVE-2022-3312, CVE-2022-3313, CVE-2022-3314, CVE-2022-3315, CVE-2022-3316, CVE-2022-3317, CVE-2022-3318

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 106.0

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://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_27.html?m=1

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

Identifikátor

TP-Link Archer AX10 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti Wi-Fi routera TP-Link Archer AX10. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.09.2022

CVE

CVE-2022-40486

Zasiahnuté systémy

TP-Link Archer AX10 vo verzii firmware 1.3.1 Build 20220401 Rel. 57450(5553) (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nebola vydaná bezpečnostná záplata, administrátorom preto odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://exchange.xforce.ibmcloud.com/vulnerabilities/237469
https://github.com/gscamelo/TP-Link-Archer-AX10-V1/blob/main/README.md

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.
Najzávažnejšie zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených UDP paketov spôsobiť zneprístupnenie služby.
Ostatné zraniteľnosti by útočníci mohli zneužiť na eskaláciu privilégií, vykonanie škodlivého kódu a neoprávnených zmien v systéme.

Dátum prvého zverejnenia varovania

28.09.2022

CVE

CVE-2022-20662, CVE-2022-20769, CVE-2022-20775, CVE-2022-20810, CVE-2022-20818, CVE-2022-20830, CVE-2022-20837, CVE-2022-20844, CVE-2022-20847, CVE-2022-20848, CVE-2022-20850, CVE-2022-20851, CVE-2022-20855, CVE-2022-20856, CVE-2022-20864, CVE-2022-20870, CVE-2022-20915, CVE-2022-20919, CVE-2022-20920, CVE-2022-20930, CVE-2022-20944, CVE-2022-20945

Zasiahnuté systémy
Cisco Catalyst 9100 Series Access Point
Cisco WLC AireOS
Cisco IOS XE
Cisco IOS
Cisco vManage
SD-WAN vBond Orchestrator Software
SD-WAN vEdge Cloud Routers
SD-WAN vEdge Routers
SD-WAN vManage Software
SD-WAN vSmart Controller Software
Catalyst 3600 Series Switches
Catalyst 3650 Series Switches
Catalyst 3800 Series Switches
Catalyst 3850 Series Switches
Catalyst 9100 Series AP
Catalyst 9200 Series Switches
Catalyst 9300 Series Switches
Catalyst 9400 Series Switches
Catalyst 9500 Series Switches
Catalyst 9600 Series Switches
Cisco Embedded Wireless Controllers
Embedded Wireless Controller on Catalyst Access Points
Catalyst 9800-CL Wireless Controllers for Cloud
Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
Catalyst 9800 Series Wireless Controllers
ASR 1000 Series Embedded Services Processors models ESP 100-X and ESP 200-X
Catalyst 8500 Series Edge Platforms models C8500-12X4QC and C8500-12X
SD-WAN vBond Orchestrator Software
SD-WAN vEdge Routers
SD-WAN vManage Software
SD-WAN vSmart Controller Software
Cisco Duo for macOS
Standalone IOS XE SD-WAN Software

Následky
Zneprístupnenie služby
Eskalácia privilégií
Vykonanie škodlivého kódu
Neoprávnená zmena v systéme

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-udp-dos-XDyEwhNz
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-mKGRrsCB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dhcp-dos-76pCjPxK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssh-excpt-dos-FzOBQTnk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mpls-dos-Ab4OUL3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-cip-dos-9rTbKLt9
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-6vpe-dos-tJBtf5Zv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewc-priv-esc-nderYLtK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-mob-dos-342YAc6J
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-assoc-dos-EgVqtON8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdinj-Gje47EMn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-cli-xkGwmqKu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-avc-NddSGB8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdavc-ZA5fpXX2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-info-disc-nrORXjO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-macOS-bypass-uKZNpXE6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cwlc-snmpidv-rnyyQzUZ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-arb-file-delete-VB2rVcQv
https://www.redpacketsecurity.com/cisco-ios-xe-denial-of-service-cve-2022-20848/

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

Identifikátor

Matrix (decentralized communication platform) - viacero bezpečnostných zraniteľností

Popis

Spoločnosť The Matrix.org Foundation vydala bezpečnostnú aktualizáciu na svoj software development kit Matrix, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi pomocou špeciálne vytvorenej správy vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

22.09.2022

CVE

CVE-2022-39246, CVE-2022-39248, CVE-2022-39249, CVE-2022-39250, CVE-2022-39251, CVE-2022-39255, CVE-2022-39257

Zasiahnuté systémy

matrix-js-sdk vo verzii staršej ako 19.7.0
matrix-ios-sdk vo verzii staršej ako 0.23.19
matrix-android-sdk2 vo verzii staršej ako 1.5.1

Následky

Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie využívajúce klomunikačný protokol Matrix nevyužívajú SDK v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.

Zdroje

https://www.bleepingcomputer.com/news/security/matrix-install-security-update-to-fix-end-to-end-encryption-flaws/
https://matrix.org/blog/2022/09/28/upgrade-now-to-address-encryption-vulns-in-matrix-sdks-and-clients
https://nvd.nist.gov/vuln/detail/CVE-2022-39251
https://nvd.nist.gov/vuln/detail/CVE-2022-39255
https://nvd.nist.gov/vuln/detail/CVE-2022-39248

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell ThinServer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt ThinManager ThinServer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej TFTP alebo HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.09.2022

CVE

CVE-2022-38742

Zasiahnuté systémy

Rockwell Automation ThinManager ThinServer vo verzii 11.0.0 až 11.0.4
Rockwell Automation ThinManager ThinServer vo verzii 11.1.0 až 11.1.4
Rockwell Automation ThinManager ThinServer vo verzii 11.2.0 až 11.2.5
Rockwell Automation ThinManager ThinServer vo verzii 12.0.0 až 12.0.2
Rockwell Automation ThinManager ThinServer vo verzii 12.1.0 až 12.1.3
Rockwell Automation ThinManager ThinServer vo verzii 13.0.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelene od Internetu.
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.cisa.gov/uscert/ics/advisories/icsa-22-270-03

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

Identifikátor

Hitachi Lumada APM Edge - bezpečnostné zraniteľnosti

Popis

Spoločnosť Hitachi Energu vydala bezpečnostnú aktualizáciu na svoj produkt Lumada APM Edge, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosi spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá, získať root prístup a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.09.2022

CVE

CVE-2022-0492

Zasiahnuté systémy

Lumada APM Edge vo verzii staršej ako 6.3

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelene od Internetu.
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-22-270-02