BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 03. 2023 - 28. 03. 2023

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
Naša značka:
01794/2022/SK-CERT-1079

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

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente WebKit, 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.
Vyššie popísaná zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi

Dátum prvého zverejnenia varovania

18.01.2023

CVE

CVE-2022-26702, CVE-2022-43551, CVE-2022-43552, CVE-2023-0049, CVE-2023-0051, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433, CVE-2023-0512, CVE-2023-23494, CVE-2023-23514, CVE-2023-23523, CVE-2023-23525, CVE-2023-23526, CVE-2023-23527, CVE-2023-23528, CVE-2023-23529, CVE-2023-23532, CVE-2023-23533, CVE-2023-23534, CVE-2023-23535, CVE-2023-23537, CVE-2023-23538, CVE-2023-23540, CVE-2023-23541, CVE-2023-23542, CVE-2023-23543, CVE-2023-27928, CVE-2023-27929, CVE-2023-27931, CVE-2023-27932, CVE-2023-27933, CVE-2023-27934, CVE-2023-27935, CVE-2023-27936, CVE-2023-27937, CVE-2023-27941, CVE-2023-27942, CVE-2023-27943, CVE-2023-27944, CVE-2023-27946, CVE-2023-27949, CVE-2023-27951, CVE-2023-27952, CVE-2023-27953, CVE-2023-27954, CVE-2023-27955, CVE-2023-27956, CVE-2023-27957, CVE-2023-27958, CVE-2023-27959, CVE-2023-27961, CVE-2023-27962, CVE-2023-27963, CVE-2023-27965, CVE-2023-27968, CVE-2023-27969, CVE-2023-27970, CVE-2023-28178, CVE-2023-28180, CVE-2023-28181, CVE-2023-28182, CVE-2023-28190, CVE-2023-28192, CVE-2023-28194, CVE-2023-28200

Zasiahnuté systémy

Apple macOS Ventura vo verzii staršej ako 13.3
Apple Safari vo verzii staršej ako 16.4
Apple Studio Display Firmware Update vo verzii staršej ako 16.4
Apple OS 15.7.4 and iPadOS vo verzii staršej ako 15.7.4
Apple tvOS vo verzii staršej ako 16.4
Apple macOS Big Sur vo verzii staršej ako 11.7.5
Apple iOS 16.4 and iPadOS vo verzii staršej ako 16.4
Apple macOS Monterey vo verzii staršej ako 12.6.4
Apple watchOS vo verzii staršej ako 9.4

Následky

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

Odporúčania
Administrátorom a používateľom odporúčame vykonať bezodkladnú aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého 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://support.apple.com/kb/HT1222 https://support.apple.com/en-us/HT201222 https://support.apple.com/en-us/HT213670 https://support.apple.com/en-us/HT213671 https://support.apple.com/en-us/HT213672 https://support.apple.com/en-us/HT213673 https://support.apple.com/en-us/HT213674 https://support.apple.com/en-us/HT213675 https://support.apple.com/en-us/HT213676 https://support.apple.com/en-us/HT213677 https://support.apple.com/en-us/HT213678 https://nvd.nist.gov/vuln/detail/CVE-2023-23529 https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20230328 https://www.cisa.gov/news-events/alerts/2023/03/28/apple-releases-security-updates-multiple-products

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 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

21.03.2023

CVE

CVE-2023-1528, CVE-2023-1529, CVE-2023-1530, CVE-2023-1531, CVE-2023-1532, CVE-2023-1533, CVE-2023-1534

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 111.0.5563.110

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/2023/03/stable-channel-update-for-desktop_21.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/250662

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

Vývojári open-source automatizačného servera Jenkins zverejnili informácie o zraniteľnostiach pluginov určených pre ich produkt.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v plugine Convert To Pipeline, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať CSRF (Cross Site Request Forgery) útoky a web cache poisoning.

Dátum prvého zverejnenia varovania

21.03.2023

CVE

CVE-2023-28668, CVE-2023-28669, CVE-2023-28670, CVE-2023-28671, CVE-2023-28672, CVE-2023-28673, CVE-2023-28674, CVE-2023-28675, CVE-2023-28676, CVE-2023-28677, CVE-2023-28678, CVE-2023-28679, CVE-2023-28680, CVE-2023-28681, CVE-2023-28682, CVE-2023-28683, CVE-2023-28684, CVE-2023-28685

Zasiahnuté systémy

JaCoCo Plugin vo verzii staršej ako 3.3.2.1
OctoPerf Load Testing Plugin Plugin vo verzii staršej ako 4.5.1
OctoPerf Load Testing Plugin Plugin vo verzii staršej ako 4.5.2
OctoPerf Load Testing Plugin Plugin vo verzii staršej ako 4.5.3
Pipeline Aggregator View Plugin vo verzii staršej ako 1.14
Role-based Authorization Strategy Plugin vo verzii staršej ako 587.588.v850a_20a_30162
AbsInt a³ Plugin vo všetkých verziách
Convert To Pipeline Plugin vo všetkých verziách
Cppcheck Plugin vo všetkých verziách
Crap4J Plugin vo všetkých verziách
Mashup Portlets Plugin vo všetkých verziách
Performance Publisher Plugin vo všetkých verziách
Phabricator Differential Plugin vo všetkých verziách
remote-jobs-view-plugin Plugin vo všetkých verziách
Visual Studio Code Metrics Plugin vo všetkých verziách

Následky

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

Odporúčania
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú uvedené pluginy v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností. 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 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. 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/2023-03-21/ https://exchange.xforce.ibmcloud.com/vulnerabilities/250631

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

Identifikátor

EY-modulo 5 Building Automation Stations - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu EY-modulo 5 Building Automation Stations.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.03.2023

CVE

CVE-2023-22300, CVE-2023-27927, CVE-2023-28650, CVE-2023-28652, CVE-2023-28655

Zasiahnuté systémy

EY-modulo 5 Building Automation Stations vo všetkých verziách

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Vzhľadom na to, že výrobca neplánuje pre dané zraniteľnosti vydať bezpečnostné záplaty, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.
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-23-082-03

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

Identifikátor

Interactive Graphical SCADA System - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoje portfólio produktov IGSS, ktorá opravuje viacero bezpečnostných zraniteľností.

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

Dátum prvého zverejnenia varovania

14.03.2023

CVE

CVE-2023-27977, CVE-2023-27978, CVE-2023-27979, CVE-2023-27980, CVE-2023-27981, CVE-2023-27982, CVE-2023-27983, CVE-2023-27984

Zasiahnuté systémy

IGSS Data Server, Dashboard and Custom Reports (RMS) vo verzii staršej ako 16.0.0.23041

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf

https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-04

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.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.
Ostatné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom alebo vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

22.03.2023

CVE

CVE-2023-20027, CVE-2023-20029, CVE-2023-20035, CVE-2023-20055, CVE-2023-20056, CVE-2023-20059, CVE-2023-20065, CVE-2023-20066, CVE-2023-20067, CVE-2023-20072, CVE-2023-20080, CVE-2023-20081, CVE-2023-20082, CVE-2023-20097, CVE-2023-20100, CVE-2023-20107, CVE-2023-20112, CVE-2023-20113

Zasiahnuté systémy
ASA 5516-X Security Appliances ASA Software ASR 1000 Series Aggregation Services Routers Business 150 APs and 151 Mesh Extenders Catalyst 8000 Edge Platforms Family Catalyst 8000V Edge Software Routers Catalyst 8200 Series Edge Platforms Catalyst 8300 Series Edge Platforms Catalyst 8500L Series Edge Platforms Catalyst 9100 APs Catalyst 9200 Series Switches Catalyst 9300 Series Switches Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches Catalyst 9800 Series Wireless Controllers Catalyst 9800-CL Wireless Controllers for Cloud Catalyst IW6300 Heavy Duty Series APs Catalyst IW9165 Heavy Duty Series Catalyst IW9165 Rugged Series Catalyst IW9167 Heavy Duty Series Cloud Services Router (CSR) 1000V Series Cloud Services Router 1000V Series DNA Center Embedded Wireless Controllers on Catalyst Access Points FTD Software Integrated AP on 1100 Integrated Services Routers IOS Software IOS XE Software SD-WAN vManage Software Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE.

Následky
Zneprístupnenie služby Neoprávnený prístup k citlivým údajom Vykonanie škodlivého kódu

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. 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv4-vfr-dos-CXxtFacb https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aironetap-cmdinj-6bjT4FL8 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa5500x-entropy-6v9bHVYP https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-apjoin-dos-nXRHkt5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-pe7zAbdR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-priv-esc-sABD8hcU https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-csrf-76RDbLEh https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-assoc-dos-D2SunWK2 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-dos-wFujBHKw https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk CVSS

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens 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 eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.03.2023

CVE

CVE-2022-32469, CVE-2022-32470, CVE-2022-32471, CVE-2022-32475, CVE-2022-32477, CVE-2022-32953, CVE-2022-32954, CVE-2022-38767

Zasiahnuté systémy

SIPROTEC 5 6MD85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 6MD86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 6MD89 (CP300) vo všetkých verziách
SIPROTEC 5 6MU85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7KE85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SA86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SA87 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SD86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SD87 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SJ85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SJ86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SK85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SL86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SL87 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SS85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7ST85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7ST86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7SX85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7UM85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7UT85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7UT86 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7UT87 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7VE85 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 7VK87 (CP300) vo verzii staršej ako V9.30
SIPROTEC 5 Communication Module ETH-BA-2EL vo verzii staršej ako V9.30

SIPROTEC 5 Communication Module ETH-BB-2FO vo verzii staršej ako V9.30
SIPROTEC 5 Communication Module ETH-BD-2FO vo verzii staršej ako V9.30
SIPROTEC 5 Compact 7SX800 (CP050) vo verzii staršej ako V9.30
RUGGEDCOM APE1808 ADM (6GK6015-0AL20-0GL0) vo všetkých verziách
RUGGEDCOM APE1808 ADM CC (6GK6015-0AL20-0GL1) vo všetkých verziách
RUGGEDCOM APE1808 CKP (6GK6015-0AL20-0GK0) vo všetkých verziách
RUGGEDCOM APE1808 CKP CC (6GK6015-0AL20-0GK1) vo všetkých verziách
RUGGEDCOM APE1808 CLOUDCONNECT (6GK6015-0AL20-0GM0) vo všetkých verziách
RUGGEDCOM APE1808 CLOUDCONNECT CC (6GK6015-0AL20-0GM1) vo všetkých verziách
RUGGEDCOM APE1808 ELAN (6GK6015-0AL20-0GP0) vo všetkých verziách
RUGGEDCOM APE1808 ELAN CC (6GK6015-0AL20-0GP1) vo všetkých verziách
RUGGEDCOM APE1808 SAM-L (6GK6015-0AL20-0GN0) vo všetkých verziách
RUGGEDCOM APE1808 SAM-L CC (6GK6015-0AL20-0GN1) vo všetkých verziách
RUGGEDCOM APE1808CLA-P (6GK6015-0AL20-1AA0) vo všetkých verziách
RUGGEDCOM APE1808CLA-P CC (6GK6015-0AL20-1AA1) vo všetkých verziách
RUGGEDCOM APE1808CLA-S1 (6GK6015-0AL20-1AB0) vo všetkých verziách
RUGGEDCOM APE1808CLA-S1 CC (6GK6015-0AL20-1AB1) vo všetkých verziách
RUGGEDCOM APE1808CLA-S3 (6GK6015-0AL20-1AD0) vo všetkých verziách
RUGGEDCOM APE1808CLA-S3 CC (6GK6015-0AL20-1AD1) vo všetkých verziách
RUGGEDCOM APE1808CLA-S5 (6GK6015-0AL20-1AF0) vo všetkých verziách
RUGGEDCOM APE1808CLA-S5 CC (6GK6015-0AL20-1AF1) vo všetkých verziách
RUGGEDCOM APE1808LNX (6GK6015-0AL20-0GH0) vo všetkých verziách
RUGGEDCOM APE1808LNX CC (6GK6015-0AL20-0GH1) vo všetkých verziách
RUGGEDCOM APE1808W10 (6GK6015-0AL20-0GJ0) vo všetkých verziách
RUGGEDCOM APE1808W10 CC (6GK6015-0AL20-0GJ1) vo všetkých verziách

Následky

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

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-080-04
https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RoboDK - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu RoboDK.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.03.2023

CVE

CVE-2023-1516

Zasiahnuté systémy

RoboDK vo verzii staršej ako v5.5.3 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne 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. 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-23-082-01

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

Identifikátor

Keysight Technologies N6854A Geolocation Server - bezpečnostná zraniteľnosť

Popis

Spoločnosť Keysight Technologies vydala bezpečnostnú aktualizáciu na svoj produkt N6854A Geolocation Server, ktorá opravuje bezpečnostnú zraniteľnosť.
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

21.03.2023

CVE

CVE-2023-1399

Zasiahnuté systémy

N6854A Geolocation server vo verzii staršej ako 2.4.3.

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.
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-23-080-01

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

Identifikátor

KVMS Pro - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu KVMS Pro.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

23.03.2023

CVE

CVE-2023-1518

Zasiahnuté systémy

KVMS Pro vo verzii staršej ako V2.01.0.T.190521

Následky

Neoprávnený prístup k citlivým údajom
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť nie sú v súčasnosti dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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-23-082-02

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

Identifikátor

Apache Tomcat - bezpečnostná zraniteľnosť

Popis

Vývojári servletu Apache Tomcat vydali bezpečnostnú aktualizáciu svojho produktu, 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 v session cookies.

Dátum prvého zverejnenia varovania

22.03.2023

CVE

CVE-2023-28708

Zasiahnuté systémy

Apache Tomcat vo verzii staršej ako 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3

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.

Zdroje

https://seclists.org/oss-sec/2023/q1/186
https://exchange.xforce.ibmcloud.com/vulnerabilities/250740

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.2**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Aruba CX switch - bezpečnostná zraniteľnosť

Popis

Spoločnosť Aruba vydala bezpečnostné aktualizácie na svoje switche série CX, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.03.2023

CVE

CVE-2023-1168

Zasiahnuté systémy

AOS-CX 10.11.xxxx vo verzii staršej ako 10.11.0001
AOS-CX 10.10.xxxx vo verzii staršej ako 10.10.1030
AOS-CX 10.06.xxxx vo verzii staršej ako 10.06.0240

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.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ABB Pulsar Plus Controller - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na produkty Infinity DC Power Plant a Pulsar Plus System Controller, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

23.03.2023

CVE

CVE-2022-1607, CVE-2022-26080

Zasiahnuté systémy

Infinity DC Power Plant a Pulsar Plus System Controller vo verzii staršej ako 5.0.0 (platí pre aplikácie aj webstránky)

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.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=9AKK108467A6732
https://www.cisa.gov/news-events/ics-advisories/icsa-23-082-05