BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 07. 2022 - 23. 08. 2022

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-868

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

Identifikátor

Apple iOS, iPadOS, macOS - dve zero-day bezpečnostné zraniteľnosti

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje dve zero-day bezpečnostné zraniteľnosti.
Najzávažnejšia zero-day 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.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

17.08.2022

CVE

CVE-2022-32893, CVE-2022-32894

Zasiahnuté systémy

iOS vo verzii staršej ako 15.6.1
iPadOS vo verzii staršej ako 15.6.
macOS vo verzii staršej ako 12.5.1

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://support.apple.com/en-us/HT213412
https://www.darkreading.com/vulnerabilities-threats/patch-apple-zero-days-exploited
https://www.helpnetsecurity.com/2022/08/18/cve-2022-32894-cve-2022-32893-cve-2022-2856/
https://www.redpacketsecurity.com/apple-ios-and-ipados-code-execution-cve-2022-32893/

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

Identifikátor

TP-Link TL-WR841N - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti smerovačov TP-Link TL-WR841N.
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

22.08.2022

CVE

CVE-2022-30024

Zasiahnuté systémy

TL-WR841 V12 vo verzii firmware 160624
TL-WR841 V11 vo verzii firmware 160325 a 150616
TL-WR841 V10 vo verzii firmware 150310

Následky

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

Odporúčania

Administrátorom 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://www.securitynewspaper.com/2022/08/22/critical-vulnerability-in-tp-link-most-sold-router-tp-link-tl-wr841/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

B&R Automation Studio 4 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu B&R Industrial Automation Studio 4.

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.

Zraniteľnosť možno zneužiť len na inštaláciách s povoleným nahrávaním projektových súborov, pričom táto funkcia nie je predvolene aktivovaná.

Dátum prvého zverejnenia varovania

16.08.2022

CVE

CVE-2021-22289

Zasiahnuté systémy

B&R Industrial Automation Studio 4 vo všetkých verziách

Následky

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

Pre dočasnú mitigáciu odporúčame postupovať podľa pokynov výrobcu uvedených na webovej adrese uvedenej v časti "zdroje".

Odporúčania

Keďže zraniteľná funkcia nie je predvolene aktivovaná, výrobca odporúča nezapínať ju.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-05

https://www.br-automation.com/downloads_br_productcatalogue/assets/1640529306294-en-original-1.0.pdf

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

Identifikátor

HPE ProLiant a HPE Synergy produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

10.08.2022

CVE

CVE-2021-33060, CVE-2022-21233

Zasiahnuté systémy

HPE ProLiant DL110 Gen10 Plus Telco server vo verzii staršej ako 1.62_07-14-2022
HPE ProLiant DL360 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022
HPE ProLiant DL380 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022
HPE ProLiant DL20 Gen10 Plus server vo verzii staršej ako 1.60_07-14-2022
HPE ProLiant ML30 Gen10 Plus server vo verzii staršej ako 1.60_07-14-2022
HPE ProLiant DX360 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022 - použite BIOS v.U46
HPE ProLiant DX380 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022 - použite BIOS v.U46
HPE ProLiant DX360 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022 - použite BIOS v.U46
HPE ProLiant DX380 Gen10 Plus server vo verzii staršej ako 1.62_07-14-2022 - použite BIOS v.U46
HPE Synergy 480 Gen10 Plus Compute Module vo verzii staršej ako 1.62_07-14-2022

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému.

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Nakoľko sa jedná o aktualizáciu UEFI BIOS, odporúčame postupovať podľa pokynov výrobcu.

Zdroje
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04341en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04342en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04345en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04346en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04347en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04356en_us

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť výskumníkmi označovanú ako DirtyCred.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.08.2022

CVE

CVE-2022-2588

Zasiahnuté systémy

cpe:2.3:o:linux:linux_kernel vo verzii staršej ako 5.10.102
cpe:2.3:o:linux:linux_kernel vo verzii staršej ako 5.15.25
cpe:2.3:o:linux:linux_kernel vo verzii staršej ako 5.16.11

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

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://access.redhat.com/security/cve/cve-2022-2588
https://thehackernews.com/2022/08/as-nasty-as-dirty-pipe-8-year-old-linux.html

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

Identifikátor

OPC UA a X80 Advanced RTU - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na komunikačné moduly Modicon OPC UA a X80 Advanced RTU, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia 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

19.08.2022

CVE

CVE-2022-34759, CVE-2022-34760, CVE-2022-34761, CVE-2022-34762, CVE-2022-34763, CVE-2022-34764, CVE-2022-34765

Zasiahnuté systémy

OPC UA Modicon Communication Module (BMENUA0100) vo verzii staršej ako V2.01
X80 Advanced RTU Communication Module (BMENOR2200H) vo verzii staršej ako V3.02.02

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-193-01_OPC_UA_X80_Advanced_RTU_Modicon_Communication_Modules_Security_Notification_V3.0.pdf&p_Doc_Ref=SEVD-2022-193-01&_ga=2.103765760.1652011725.1661159793-1407605564.1661159793

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

Identifikátor

Free IPA - bezpečnostná zraniteľnosť

Popis

Spoločnosť RedHat vydala bezpečnostnú aktualizáciu na svoj open source systém pre manažment identít Free IPA, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

19.08.2022

CVE

CVE-2022-2414

Zasiahnuté systémy

Red Hat Enterprise Linux 6-9
Red Hat Certificate System 9 a 10

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://portswigger.net/daily-swig/vulnerability-in-open-source-identity-management-system-free-ipa-could-lead-to-xxe-attacks
https://nvd.nist.gov/vuln/detail/CVE-2022-2414

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

LS ELECTRIC PLC a XG5000 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti riadiacich systémov LS ELECTRIC PLC a XG5000.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup do systému a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.08.2022

CVE

CVE-2022-2758

Zasiahnuté systémy

LS Electric PLC vo všetkých verziách
XG5000 vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené 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-22-228-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Yokogawa CENTUM Controller FCS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Yokogawa vydala bezpečnostnú aktualizáciu na svoje portfólio produktov CENTUM VP & CS 3000 Controller FCS, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.08.2022

CVE

CVE-2022-33939

Zasiahnuté systémy

CENTUM CS 3000 vo všetkých verziách
CENTUM CS 3000 Entry Class vo všetkých verziách
CENTUM VP vo všetkých verziách
CENTUM VP Entry Class vo všetkých verziách
CENTUM VP vo verzii staršej ako R5.04.20
CENTUM VP Entry Class vo verzii staršej ako R6.03.00

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-228-01
https://web-material3.yokogawa.com/1/33029/files/YSAR-22-0008-E.pdf