BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 11. 2022 - 08. 11. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apple Xcode - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Cisco Identity Services Engine - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Nokia ASIK AirScale System Module - tri bezpečnostné zraniteľnosti	Vysoká	**8.4**
04.	OpenHarmony - tri bezpečnostné zraniteľnosti	Vysoká	**8.4**
05.	Cisco BroadWorks CommPilot Application - dve bezpečnostné zraniteľnosti	Vysoká	**8.3**
06.	Delta Industrial Automation DIALink - bezpečnostná zraniteľnosť	Vysoká	**8.1**

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-931

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

Identifikátor

Apple Xcode - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na svoje integrované vývojárske prostredie Xcode, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia 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.

Dátum prvého zverejnenia varovania

08.10.2022

CVE

CVE-2022-29187, CVE-2022-39253, CVE-2022-39260, CVE-2022-42797

Zasiahnuté systémy

Xcode vo verzii staršej ako 14.1

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://access.redhat.com/security/cve/cve-2022-39260#cve-cvss-v3
https://support.apple.com/en-us/HT213496

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

Identifikátor

Cisco Identity Services Engine - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Identity Services Engine, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom CSRF(Cross Site Request Forgery) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.11.2022

CVE

CVE-2022-20961

Zasiahnuté systémy

Cisco ISE 2.6 vo verzii staršej ako 2.6p12
Cisco ISE 2.7 vo verzii staršej ako 2.7p8
Cisco ISE 3.0 vo verzii staršej ako 3.0p6
Cisco ISE 3.1 vo verzii staršej ako 3.1p4

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Nokia ASIK AirScale System Module - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach systémového modulu Nokia ASIK AirScale.
Najzávažnejšie zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov alokálny, autentifikovaný útočník s právomocami používateľa by ich mohol zneužiť na vykonanie škodlivého kódu a narušenie integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.11.2022

CVE

CVE-2022-2482, CVE-2022-2483, CVE-2022-2484

Zasiahnuté systémy

Nokia ASIK AirScale vo verzii staršej ako ASIK 474021A.102 (vrátane)

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Spoločnosť Nokia vydala technický sumár obsahujúci inštrukcie ohľadom mitigácie dopadu uvedených zraniteľností na adrese https://customer.nokia.com/support/s/
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/uscert/ics/advisories/icsa-22-307-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

OpenHarmony - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach open-source projektu OpenHarmony. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom techniky path traversal spôsobiť narušenie dôvernosti, integrity a dostupnosti systému. V kombinácii s ostatnými zraniteľnosťami môže dôjsť k úniku zo sandboxu, neautorizovanému prístupu do systému a eskalácii privilégií.

Dátum prvého zverejnenia varovania

06.11.2022

CVE

CVE-2022-43449, CVE-2022-43451, CVE-2022-43495

Zasiahnuté systémy

OpenHarmony vo verzii staršej ako v3.1.2-Release (vrátane)

Následky

Eskalácia privilégií
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 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://gitee.com/openharmony/security/blob/master/en/security-disclosure/2022/2022-11.md
https://nvd.nist.gov/vuln/detail/CVE-2022-43451

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

Identifikátor

Cisco BroadWorks CommPilot Application - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt BroadWorks, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia kritická bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

02.11.2022

CVE

CVE-2022-20951, CVE-2022-20958

Zasiahnuté systémy

Cisco BroadWorks CommPilot Application 23.0 vo všetkých verziách
Cisco BroadWorks CommPilot Application 23.0 vo verzii staršej ako CommPilot-23 version 2022.10_1.313
Cisco BroadWorks CommPilot Application 24.0 vo verzii staršej ako CommPilot-24 version 2022.10_1.313
Cisco BroadWorks CommPilot Application 25.0 vo verzii staršej ako CommPilot-25 version 2022.10_1.313

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-ssrf-BJeQfpp

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

Identifikátor

Delta Industrial Automation DIALink - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Industrial Automation vydala bezpečnostnú aktualizáciu na svoj edge server box DIALink, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.11.2022

CVE

CVE-2022-2969

Zasiahnuté systémy

DIALink vo verzii staršej ako v1.5.0.0 Beta 4

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://thehackernews.com/2022/11/cisa-warns-of-critical-vulnerabilities.html
https://www.cisa.gov/uscert/ics/advisories/icsa-22-307-03