BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 01. 2024 - 09. 01. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Kofax Power PDF - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Qnap produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Inductive Automation Ignition - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	NEXO-OS V1500-SP2 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	ChromeOS a ChromeOS Flex - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	SolarWinds Access Rights Manager - bezpečnostná zraniteľnosť	Vysoká	**8.6**
07.	IBM Db2 - bezpečnostná zraniteľnosť	Vysoká	**8.4**
08.	X.Org Server - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
09.	Bentley View a MicroStation - bezpečnostná zraniteľnosť	Vysoká	**7.8**
10.	Apache Axis - bezpečnostná zraniteľnosť	Vysoká	**7.5**
11.	Postfix, Sendmail, Exim, Cisco Secure Email, MS Exchange - bezpečnostná zraniteľnosť	Stredná	**4.3**

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-1460

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

Identifikátor

Kofax Power PDF - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Kofax vydala bezpečnostnú aktualizáciu na svoj produkt Kofax Power PDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.01.2024

CVE

CVE-2023-51563, CVE-2023-51564, CVE-2023-51565, CVE-2023-51566, CVE-2023-51567, CVE-2023-51568, CVE-2023-51569

Zasiahnuté systémy

Kofax Power PDF Advanced vo verzii staršej ako 5.0.0 Fix Pack 16

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

http://docshield.kofax.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.16.htm
https://www.zerodayinitiative.com/advisories/ZDI-24-007/
https://www.zerodayinitiative.com/advisories/ZDI-24-006/
https://www.zerodayinitiative.com/advisories/ZDI-24-005/
https://www.zerodayinitiative.com/advisories/ZDI-24-004/
https://www.zerodayinitiative.com/advisories/ZDI-24-003/
https://www.zerodayinitiative.com/advisories/ZDI-24-002/
https://www.zerodayinitiative.com/advisories/ZDI-24-001/

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

Identifikátor

Qnap produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Qnap vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Video Station, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.01.2023

CVE

CVE-2022-43634, CVE-2023-39294, CVE-2023-39296, CVE-2023-41287, CVE-2023-41288, CVE-2023-41289, CVE-2023-45039, CVE-2023-45040, CVE-2023-45041, CVE-2023-45042, CVE-2023-45043, CVE-2023-45044, CVE-2023-47219, CVE-2023-47559, CVE-2023-47560

Zasiahnuté systémy

QTS vo verzii staršej ako 5.1.3.2578 build 20231110
QuTS hero vo verzii staršej ako h5.1.3.2578 build 20231110
Video Station vo verzii staršej ako 5.7.2 (2023/11/23)
QuMagie vo verzii staršej ako 2.2.1
QcalAgent vo verzii staršej ako 1.1.8

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.qnap.com/uploads/security-advisories/QSA-23-55/CVE-2023-41288.json
https://www.qnap.com/en/security-advisory/qsa-23-27
https://www.qnap.com/en/security-advisory/qsa-23-22
https://www.qnap.com/en/security-advisory/qsa-23-55
https://www.qnap.com/en/security-advisory/qsa-23-32
https://www.qnap.com/en/security-advisory/qsa-23-23
https://www.qnap.com/en/security-advisory/qsa-23-54
https://www.qnap.com/en/security-advisory/qsa-23-64
https://www.qnap.com/en/security-advisory/qsa-23-34
https://www.qnap.com/en/security-advisory/qsa-23-54
https://www.qnap.com/en/security-advisory/qsa-23-64

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

Identifikátor

Inductive Automation Ignition - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Inductive Automation vydala bezpečnostnú aktualizáciu na svoj produkt Ignition, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód v kontexte používateľa SYSTEM s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.01.2023

CVE

CVE-2023-50219, CVE-2023-50220, CVE-2023-50221, CVE-2023-50222, CVE-2023-50223

Zasiahnuté systémy

Inductive Automation Ignition vo verzii staršej ako 8.1.35

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://security.inductiveautomation.com/?tcuUid=fc4c4515-046d-4365-b688-693337449c5b
https://www.zerodayinitiative.com/advisories/ZDI-24-014/
https://www.zerodayinitiative.com/advisories/ZDI-24-015/
https://www.zerodayinitiative.com/advisories/ZDI-24-016/
https://www.zerodayinitiative.com/advisories/ZDI-24-017/
https://www.zerodayinitiative.com/advisories/ZDI-24-018/

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

Identifikátor

NEXO-OS V1500-SP2 - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu NEXO-OS V1500-SP2.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.01.2024

CVE

CVE-2023-48242, CVE-2023-48243, CVE-2023-48244, CVE-2023-48245, CVE-2023-48246, CVE-2023-48247, CVE-2023-48248, CVE-2023-48249, CVE-2023-48250, CVE-2023-48251, CVE-2023-48252, CVE-2023-48253, CVE-2023-48254, CVE-2023-48255, CVE-2023-48256, CVE-2023-48257, CVE-2023-48258, CVE-2023-48259, CVE-2023-48260, CVE-2023-48261, CVE-2023-48262, CVE-2023-48263, CVE-2023-48264, CVE-2023-48265, CVE-2023-48266

Zasiahnuté systémy

NEXO-OS vo verzii staršej ako V1500-SP2 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

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.

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-711465.html

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

Identifikátor

ChromeOS a ChromeOS Flex - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na produkty ChromeOS a ChromeOS Flex, ktoré opravujú 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

08.01.2024

CVE

CVE-2023-39191, CVE-2023-6508, CVE-2023-6509, CVE-2023-6511, CVE-2023-7024

Zasiahnuté systémy

ChromeOS a ChromeOS Flex vo verzii staršej ako 120.0.6099.203

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/2024/01/stable-channel-update-for-chromeos.html

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

Identifikátor

SolarWinds Access Rights Manager - bezpečnostná zraniteľnosť

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt Access Rights Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi obísť RabbitMQ autentifikáciu a získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.01.2024

CVE

CVE-2023-40058

Zasiahnuté systémy

Access Rights Manager (ARM) vo verzii staršej ako 2023.2.2

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

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-24-008/

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

Identifikátor

IBM Db2 - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Db2, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi zneužitím MSI repair funkcie eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.01.2023

CVE

CVE-2023-47145

Zasiahnuté systémy

IBM Db2 vo verzii staršej ako V10.5 FP11
IBM Db2 vo verzii staršej ako V11.1.4 FP7
IBM Db2 vo verzii staršej ako V11.5.9

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.ibm.com/support/pages/node/7105500
https://exchange.xforce.ibmcloud.com/vulnerabilities/270402

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

Identifikátor

X.Org Server - viacero bezpečnostných zraniteľností

Popis

Vývojári implementácie X.Org X server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom pretečenia zásobníka eskalovať svoje privilégiá a následne vykonať škodlivý kód v kontexte používateľa ROOT s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.01.2023

CVE

CVE-2023-5367, CVE-2023-6377, CVE-2023-6478

Zasiahnuté systémy

xorg-server vo verzii staršej ako 21.1.9
xwayland vo verzii staršej ako 23.2.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

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://lists.x.org/archives/xorg-announce/2023-October/003430.html
https://www.zerodayinitiative.com/advisories/ZDI-24-012/
https://www.zerodayinitiative.com/advisories/ZDI-24-011/
https://www.zerodayinitiative.com/advisories/ZDI-24-010/
https://www.zerodayinitiative.com/advisories/ZDI-24-009/

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

Identifikátor

Bentley View a MicroStation - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bentley Systems vydala bezpečnostnú aktualizáciu na svoje produkty MicroStation a Bentley View, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.01.2024

CVE

CVE-2023-44430

Zasiahnuté systémy

MicroStation vo verzii staršej ako 10.17.01.58
Bentley View vo verzii staršej ako 10.17.01.19

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.bentley.com/advisories/be-2022-0019/
https://www.zerodayinitiative.com/advisories/ZDI-24-019/

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

Identifikátor

Apache Axis - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Apache Axis vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.01.2024

CVE

CVE-2023-51441

Zasiahnuté systémy

Apache Axis 1.3 (vrátane)

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2024/q1/12
https://exchange.xforce.ibmcloud.com/vulnerabilities/278665

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Postfix, Sendmail, Exim, Cisco Secure Email, MS Exchange - bezpečnostná zraniteľnosť

Popis

Vývojári mailových serverov Postfix, Sendmail a Exim, ako aj spoločnosť Microsoft pre svoj mailový server MS Exchange vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť (jedná sa o totožnú zraniteľnosť v SMT protokole, v každej implementácii má však vlastný identifikátor CVE).

Spoločnosť Cisco za účelom mitigácie predmetnej zraniteľnosti vydala odporúčané nastavenia pre svoj produkt Secure Email.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi pomocou injektovanej FROM adresy zmeniť hlavičku e-mailu a vykonať spoofing útok, obchádzajúc bezpečnostné prvky ako SPF, DKIM a DMARC.

Vzhľadom na riziko využitia predmetnej zraniteľnosti pri pokročilých phishing útokoch ju uvádzame aj napriek nižšiemu CVSS hodnoteniu.

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

Dátum prvého zverejnenia varovania

04.01.2023

CVE

CVE-2023-51764, CVE-2023-51765, CVE-2023-51766

Zasiahnuté systémy

Postfix vo verzii staršej ako 3.8.4, 3.7.9, 3.6.13, 3.5.23
Sendmail vo verzii staršej ako 8.18.0.2
Exim vo verzii staršej ako 4.98, 4.97.1
Microsoft Exchange vo verzii staršej ako Október 2023
Cisco Secure Email vo všetkých verziách

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Tiež odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, detailné inštrukcie môžete nájsť na odkazoch v sekcii ZDROJE.

Zdroje
https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_1/2024
https://nvd.nist.gov/vuln/detail/CVE-2023-51766
https://nvd.nist.gov/vuln/detail/CVE-2023-51765
https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/
https://www.postfix.org/smtp-smuggling.html