BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 09. 2023 - 19. 09. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Foxit PDF Reader a Editor - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Microsoft produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	N-Able Take Control Agent - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Rockwell Automation Pavilion8 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	Apache Airflow - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	FortiWeb, FortiProxy a FortiOS - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
08.	Siemens SIMATIC a Spectrum Power - dve bezpečnostné zraniteľnosti	Vysoká	**8.2**
09.	Notepad++ - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	OPSWAT MetaDefender KIOSK - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
11.	Zoom produkty - tri bezpečnostné zraniteľnosti	Vysoká	**7.2**

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-1327

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

Identifikátor

Adobe produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch Acrobat a Reader, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2023-26369, CVE-2023-29305, CVE-2023-29306, CVE-2023-38214, CVE-2023-38215

Zasiahnuté systémy

Adobe Experience Manager (AEM) vo verzii staršej ako 6.5.18.0 alebo AEM Cloud Service Release 2023.8
Acrobat DC vo verzii staršej ako 23.003.20284
Acrobat Reader DC vo verzii staršej ako 23.003.20284
Acrobat 2020 vo verzii staršej ako 20.005.30516 (Mac) a 20.005.30514 (Win)
Acrobat Reader 2020 vo verzii staršej ako 20.005.30516 (Mac) a 20.005.30514 (Win)
Adobe Connect vo verzii staršej ako 12.4.1

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

Zdroje

https://helpx.adobe.com/security/products/experience-manager/apsb23-43.html
https://helpx.adobe.com/security/products/acrobat/apsb23-34.html
https://helpx.adobe.com/security/products/connect/apsb23-33.html

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

Identifikátor

Foxit PDF Reader a Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostnú aktualizáciu na svoje produkty Foxit PDF Reader a Foxit PDF Editor, ktorá opravuje viacero bezpečnostných zraniteľností.
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.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2023-42089, CVE-2023-42090, CVE-2023-42091, CVE-2023-42092, CVE-2023-42093, CVE-2023-42094, CVE-2023-42095, CVE-2023-42096, CVE-2023-42097, CVE-2023-42098

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 2023.2
Foxit PDF Editor vo verzii staršej ako 2023.2

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://www.zerodayinitiative.com/advisories/ZDI-23-1430/
https://www.foxit.com/support/security-bulletins.html

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

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

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Azure DevOps, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2022-41303, CVE-2023-29332, CVE-2023-33136, CVE-2023-35355, CVE-2023-36736, CVE-2023-36739, CVE-2023-36740, CVE-2023-36742, CVE-2023-36744, CVE-2023-36745, CVE-2023-36756, CVE-2023-36757, CVE-2023-36758, CVE-2023-36759, CVE-2023-36760, CVE-2023-36761, CVE-2023-36762, CVE-2023-36763, CVE-2023-36764, CVE-2023-36765, CVE-2023-36766, CVE-2023-36767, CVE-2023-36770, CVE-2023-36771, CVE-2023-36772, CVE-2023-36773, CVE-2023-36777, CVE-2023-36788, CVE-2023-36792, CVE-2023-36793, CVE-2023-36794, CVE-2023-36796, CVE-2023-36799, CVE-2023-36800, CVE-2023-36801, CVE-2023-36802, CVE-2023-36803, CVE-2023-36804, CVE-2023-36805, CVE-2023-36886, CVE-2023-38139, CVE-2023-38140, CVE-2023-38141, CVE-2023-38142, CVE-2023-38143, CVE-2023-38144, CVE-2023-38146, CVE-2023-38147, CVE-2023-38148, CVE-2023-38149, CVE-2023-38150, CVE-2023-38152, CVE-2023-38155, CVE-2023-38156, CVE-2023-38160, CVE-2023-38161, CVE-2023-38162, CVE-2023-38163, CVE-2023-38164, CVE-2023-39956, CVE-2023-41764, CVE-2023-4761, CVE-2023-4762, CVE-2023-4763, CVE-2023-4764, CVE-2023-4863

Zasiahnuté systémy

Microsoft Azure Kubernetes Service
Azure DevOps
Windows Cloud Files Mini Filter Driver
Microsoft Identity Linux Broker
3D Viewer
3D Viewer
Visual Studio Code
Microsoft Exchange Server
Microsoft Exchange Server
Microsoft Exchange Server
Microsoft Exchange Server
Visual Studio
Visual Studio
3D Viewer
Microsoft Office Word
Microsoft Office Word
Microsoft Office Outlook

Microsoft Office SharePoint
Microsoft Office
Microsoft Office Excel
Microsoft Office
3D Builder
3D Builder
3D Builder
3D Builder
Microsoft Exchange Server
.NET Framework
.NET and Visual Studio
.NET and Visual Studio
.NET and Visual Studio
.NET and Visual Studio
.NET Core & Visual Studio
Microsoft Dynamics Finance & Operations
Windows DHCP Server
Microsoft Streaming Service
Windows Kernel
Windows GDI
Windows Scripting
Microsoft Dynamics
Windows Kernel
Windows Kernel
Windows Kernel
Windows Kernel
Windows Common Log File System Driver
Windows Common Log File System Driver
Windows Themes
Microsoft Windows Codecs Library
Windows Internet Connection Sharing (ICS)
Windows TCP/IP
Windows Kernel
Windows DHCP Server
Azure DevOps
Azure HDInsights
Windows TCP/IP
Windows GDI
Windows DHCP Server
Windows Defender
Microsoft Dynamics
Microsoft Office

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

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://msrc.microsoft.com/update-guide/releaseNote/2023-Sep

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

Identifikátor

N-Able Take Control Agent - bezpečnostná zraniteľnosť

Popis

Spoločnosť N-Able vydala bezpečnostnú aktualizáciu na svoj produkt Take Control Agent, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia symbolického odkazu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.09.2023

CVE

CVE-2023-27470

Zasiahnuté systémy

N-Able Take Control Agent vo verzii staršej ako 7.0.43

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.

Zdroje

https://github.com/mandiant/Vulnerability-Disclosures/blob/master/2023/MNDT-2023-0011.md

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

Identifikátor

Rockwell Automation Pavilion8 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Pavilion8, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.09.2023

CVE

CVE-2023-29463

Zasiahnuté systémy

Pavilion8 vo verzii staršej ako 5.20

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.
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-23-257-07
https://exchange.xforce.ibmcloud.com/vulnerabilities/266099

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

Identifikátor

Apache Airflow - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Apache Airflow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

14.09.2023

CVE

CVE-2023-41267

Zasiahnuté systémy

Apache Airflow HDFS Provider vo verzii staršej ako 4.1.1

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://exchange.xforce.ibmcloud.com/vulnerabilities/266094

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

Identifikátor

FortiWeb, FortiProxy a FortiOS - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť FortiGuard vydala bezpečnostné aktualizácie na produkty FortiWeb, FortiProxy a FortiOS, ktoré opravujú dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produktoch FortiProxy a FortiOS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.09.2023

CVE

CVE-2023-29183, CVE-2023-34984

Zasiahnuté systémy

FortiProxy vo verzii staršej ako 7.2.5
FortiProxy vo verzii staršej ako 7.0.11
FortiOS vo verzii staršej ako 7.4.0
FortiOS vo verzii staršej ako 7.2.5
FortiOS vo verzii staršej ako 7.0.12
FortiOS vo verzii staršej ako 6.4.13
FortiOS vo verzii staršej ako 6.2.15
FortiWeb vo verzii staršej ako 7.2.2
FortiWeb vo verzii staršej ako 7.0.7

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.fortiguard.com/psirt/FG-IR-23-068
https://www.fortiguard.com/psirt/FG-IR-23-106

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

Identifikátor

Siemens SIMATIC a Spectrum Power - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na produkty SIMATIC a Spectrum Power, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Spectrum Power, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.09.2023

CVE

CVE-2023-38557, CVE-2023-38558

Zasiahnuté systémy

Spectrum Power 7 vo verzii staršej ako V23Q3
SIMATIC PCS neo (Administration Console) V4.0 Update 1 vo verzii bez Security Patch 01
SIMATIC PCS neo (Administration Console) V4.0 vo verzii bez Security Patch 01

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://cert-portal.siemens.com/productcert/html/ssa-646240.html
https://cert-portal.siemens.com/productcert/html/ssa-357182.html

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

Identifikátor

Notepad++ - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Notepad++.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

31.08.2023

CVE

CVE-2023-40031, CVE-2023-40036, CVE-2023-40164, CVE-2023-40166

Zasiahnuté systémy

Notepad++ vo verzii staršej ako 8.5.7

Následky

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

Odporúčania

Administrátorom 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://securitylab.github.com/advisories/GHSL-2023-092_Notepad__/
https://nvd.nist.gov/vuln/detail/CVE-2023-40031
https://www.bleepingcomputer.com/news/security/notepad-plus-plus-857-released-with-fixes-for-four-security-vulnerabilities/

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

Identifikátor

OPSWAT MetaDefender KIOSK - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť OPSWAT vydala bezpečnostnú aktualizáciu na svoj produkt MetaDefender KIOSK, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených súborov eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.09.2023

CVE

CVE-2023-36657, CVE-2023-36658, CVE-2023-36659

Zasiahnuté systémy

OPSWAT MDKIOSK 4.5.0 vo verzii staršej ako 4.6.2
OPSWAT OMVA 2.0.0 vo verzii staršej ako 2.0.7

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://docs.opswat.com/mdkiosk/release-notes/cve-2023-36658
https://exchange.xforce.ibmcloud.com/vulnerabilities/266137
https://exchange.xforce.ibmcloud.com/vulnerabilities/266138
https://exchange.xforce.ibmcloud.com/vulnerabilities/266134

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

Identifikátor

Zoom produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoom vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2023-39201, CVE-2023-39208, CVE-2023-39215

Zasiahnuté systémy

Zoom Desktop Client pre Windows vo verzii staršej ako 5.15.5
Zoom Desktop Client pre macOS vo verzii staršej ako 5.15.5
Zoom Desktop Client pre Linux vo verzii staršej ako 5.15.10
Zoom VDI Client vo verzii staršej ako 5.14.12
Zoom VDI Client vo verzii staršej ako 5.15.4
Zoom Mobile App pre Android vo verzii staršej ako 5.15.5
Zoom Mobile App pre iOS vo verzii staršej ako 5.15.5
Zoom Meeting SDK's vo verzii staršej ako 5.15.5
CleanZoom vo verzii súborov staršej ako 07/24/2023

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

Zdroje

https://explore.zoom.us/en/trust/security/security-bulletin/