BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 06. 2021 - 15. 06. 2021

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:
01439/2020/SK-CERT-451

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

Identifikátor

Johnson Controls Metasys Servers, Engines a SCT Tools - bezpečnostná zraniteľnosť

Popis

Spoločnosť Johnson Controlsvydala bezpečnostnú aktualizáciu na produkt Metasys, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

10.06.2021

CVE

-

Zasiahnuté systémy

Metasys vo verzii staršej ako 11.0.1.

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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-159-01
https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2021/jci-psa-2021-05-metasys-web.pdf?la=en&hash=B95087F18EB75E67F47942FAFEE5B01BC617FA0C

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.5**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell Automation FactoryTalk Services Platform- bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na produkt FactoryTalk Services Platform, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, 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

15.06.2021

CVE

CVE-2021-32960

Zasiahnuté systémy

FactoryTalk Services Platform vo verzii staršej ako v6.20

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.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-161-01

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia 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. Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

08.06.2021

CVE

CVE-2021-21224, CVE-2021-28550, CVE-2021-31174, CVE-2021-31178, CVE-2021-31179, CVE-2021-31199, CVE-2021-31201, CVE-2021-31939, CVE-2021-31955, CVE-2021-31956, CVE-2021-31957, CVE-2021-31959, CVE-2021-31963, CVE-2021-31968, CVE-2021-31978, CVE-2021-31985, CVE-2021-33739, CVE-2021-33742

Zasiahnuté systémy

Microsoft DWM Core Library
Microsoft SharePoint Server
Microsoft Defender
Windows Kernel
Windows NTFS
Windows MSHTML Platform
Microsoft Enhanced Cryptographic Provider
Microsoft Office Remote
Microsoft Excel
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://msrc.microsoft.com/update-guide

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/en-US/vulnerability/CVE-2021-33739
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31963
https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2021-patch-tuesday-fixes-6-exploited-zero-days-50-flaws/
https://msrc.microsoft.com/update-guide
https://threatpost.com/microsoft-patch-tuesday-in-the-wild-exploits/166724/
https://thehackernews.com/2021/06/new-uaf-vulnerability-affecting.html

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

Identifikátor

AGG Software Web Server - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť AGG Software vydala bezpečnostnú aktualizáciu na produkt Web Server, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.06.2021

CVE

CVE-2021-32962, CVE-2021-32964

Zasiahnuté systémy

AGG Web Server vo verzii staršej ako v4.0.42 Build 512

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-161-02

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

Identifikátor

Akkadian Provisioning Manager - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Akkadian Provisioning Manager. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

11.06.2021

CVE

CVE-2021-31579, CVE-2021-31580, CVE-2021-31581, CVE-2021-31582

Zasiahnuté systémy

Akkadian Provisioning Manager vo verzii staršej ako 4.50.18 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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.
Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN).

Zdroje

https://www.rapid7.com/blog/post/2021/06/08/akkadian-provisioning-manager-multiple-vulnerabilities-disclosure/
https://www.akkadianlabs.com/products/akkadian-provisioning-manager/
https://threatpost.com/unpatched-bugs-provisioning-cisco-uc/166882/

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

Identifikátor

Open Design Alliance Drawings SDK - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Open Design Alliance vydala bezpečnostnú aktualizáciu na produkt Drawings SDK, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.06.2021

CVE

CVE-2021-32936, CVE-2021-32938, CVE-2021-32940, CVE-2021-32944, CVE-2021-32946, CVE-2021-32948, CVE-2021-32950, CVE-2021-32952

Zasiahnuté systémy

Drawings SDK vo verzii staršej ako 2022.5

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-159-02
https://www.opendesign.com/security-advisories

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

Identifikátor

Schneider Electric IGSS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na produkt IGSS (Interactive Graphical SCADA System), ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvorených súborov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.06.2021

CVE

CVE-2021-22750, CVE-2021-22751, CVE-2021-22752, CVE-2021-22753, CVE-2021-22754, CVE-2021-22755, CVE-2021-22756, CVE-2021-22757, CVE-2021-22758, CVE-2021-22759, CVE-2021-22760, CVE-2021-22761, CVE-2021-22762

Zasiahnuté systémy

IGSS Definition (Def.exe) vo verzii staršej ako v15.0.0.21141

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-159-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-04