BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 11. 2020 - 10. 11. 2020

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-267

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

Identifikátor

Zraniteľnosti v produktoch OSIsoft PI Vision a PI Interface

Popis

Spoločnosť OSIsoft vydala bezpečnostné aktualizácie na svoje produkty PI Vision a PI Interface, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

10.11.2020

CVE

CVE-2013-0006, CVE-2020-25163

Zasiahnuté systémy

OSIsoft PI Interface OPC XML-DA všetky verzie staršie ako 1.7.3.x
OSIsoft PI Vision všetky verzie staršie ako 2020

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://us-cert.cisa.gov/ics/advisories/icsa-20-315-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-01

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

Identifikátor

Zraniteľnosti modulu XOOPS XooNIps

Popis

Spoločnosť XOOPS vydala bezpečnostnú aktualizáciu na svoj modul XooNIps, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje neautentifikovanému vzdialenému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.11.2020

CVE

CVE-2020-5659, CVE-2020-5662, CVE-2020-5663, CVE-2020-5664

Zasiahnuté systémy

XOOPS XooNIps verzie staršie ako 3.50

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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://jvn.jp/en/vu/JVNVU92053563/index.html

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

Identifikátor

Viacero zraniteľností v Apple produktoch

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty iOS, iPadOS, tvOS, macOS a watchOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza v jadre macOS a umožňuje lokálnemu autentifikovanému útočníkovi vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Viaceré zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

05.11.2020

CVE

CVE-2020-10002, CVE-2020-10003, CVE-2020-10004, CVE-2020-10010, CVE-2020-10011, CVE-2020-10016, CVE-2020-10017, CVE-2020-13524, CVE-2020-27902, CVE-2020-27905, CVE-2020-27909, CVE-2020-27910, CVE-2020-27911, CVE-2020-27912, CVE-2020-27916, CVE-2020-27917, CVE-2020-27918, CVE-2020-27925, CVE-2020-27926, CVE-2020-27927, CVE-2020-27929, CVE-2020-27930, CVE-2020-27932, CVE-2020-27950, CVE-2020-9974

Zasiahnuté systémy

Apple macOS Catalina verzie staršie ako 10.15.7
Apple watchOS verzie staršie ako 5.3.9
Apple watchOS verzie staršie ako 6.2.9
Apple iOS verzie staršie ako 12.4.9
Apple tvOS verzie staršie ako 4.2
Apple iOS verzie staršie ako 14.2
Apple iPadOS verzie staršie ako 14.2
Apple watchOS verzie staršie ako 7.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľnosti, 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://us-cert.cisa.gov/ncas/current-activity/2020/11/06/apple-releases-security-updates-multiple-products
https://support.apple.com/en-us/HT211947
https://support.apple.com/en-us/HT211945
https://support.apple.com/en-us/HT211944
https://support.apple.com/en-us/HT211940
https://support.apple.com/en-us/HT211930
https://support.apple.com/en-us/HT211929
https://support.apple.com/en-us/HT211928

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

Identifikátor

Bezpečnostná zraniteľnosť v PLC simulátore Schneider Electric pre EcoStruxure Control Expert

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj PLC simulátor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky cez Modbus vykonať zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.11.2020

CVE

CVE-2020-7538

Zasiahnuté systémy

PLC Simulator pre EcoStruxure Control Expert všetky verzie
PLC Simulator pre Unity Pro (predošlý názov - EcoStruxure Control Expert) všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-315-03

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť modulu Mitsubishi Electric Melsec iQ-R

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoj modul Melsec iQ-R, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.11.2020

CVE

CVE-2020-5666

Zasiahnuté systémy

Mitsubishi Electric MELSEC iQ-R R00/01/02CPU verzie staršie ako 20
Mitsubishi Electric MELSEC iQ-R R04/08/16/32/120(EN)CPU firmware verzie 52

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-317-01

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

Identifikátor

Zraniteľnosť v produktoch BD Alaris PC Unit a System Manager

Popis

Spoločnosť BD Alaris vydala bezpečnostné aktualizácie na svoje produkty PC Unity a System Manager, ktoré opravujú bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.11.2020

CVE

CVE-2020-25165

Zasiahnuté systémy

BD Alaris PC Unit, Model 8015, verzie staršie ako 9.33.1 (vrátane)
BD Alaris Systems Manager, verzie staršie ako 4.33 (vrátane)

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať webstránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-20-317-01