BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 08. 2019 - 03. 09. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Datalogic AV7000 Linear Barcode Scanner zraniteľnosť	Vysoká	**8.8**
02.	Autodesk Design Review zraniteľnosti	Vysoká	**8.8**
03.	Check Point Endpoint Security Initial Client zraniteľnosť	Vysoká	**7.8**
04.	Trend Micro Password Manager zraniteľnosti	Vysoká	**7.8**
05.	Kea zraniteľnosti	Stredná	**6.5**

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:
01380/2019/TS/OKB-213

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

Identifikátor

Datalogic AV7000 Linear Barcode Scanner zraniteľnosť

Popis

Spoločnosť Datalogic vydala bezpečnostnú aktualizáciu na svoj produkt AV7000, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi obísť autentifikačné mechanizmy a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.08.2019

CVE

CVE-2019-13526

Zasiahnuté systémy

Datalogic AV7000 Linear Barcode Scanner verzie staršie ako 4.6.0.0

Následky

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

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://www.us-cert.gov/ics/advisories/icsa-19-239-02

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

Identifikátor

Autodesk Design Review zraniteľnosti

Popis

Spoločnosť Autodesk vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených DWF a DWG súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.08.2019

CVE

CVE-2019-7362, CVE-2019-7363, CVE-2019-7364

Zasiahnuté systémy

Autodesk Design Review
Autodesk Advance Steel
Autodesk Civil 3D
Autodesk AutoCAD
Autodesk AutoCAD LT
Autodesk AutoCAD P&ID
Autodesk AutoCAD based specialized toolsets including: AutoCAD Architecture; AutoCAD Electrical; AutoCAD Map 3D; AutoCAD Mechanical; AutoCAD MEP; AutoCAD Plant 3D

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a prílohy z neznámych zdrojov.
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.autodesk.com/trust/security-advisories/adsk-sa-2019-0002
https://nvd.nist.gov/vuln/detail/CVE-2019-7363

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

Identifikátor

Check Point Endpoint Security Initial Client zraniteľnosť

Popis

Spoločnosť Check Point vydala bezpečnostnú aktualizáciu na svoj produkt Endpoint Security Initial Client, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

27.08.2019

CVE

CVE-2019-8461

Zasiahnuté systémy

Check Point Endpoint Security Initial Client for Windows verzie staršie ako E81.30

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.bleepingcomputer.com/news/security/check-point-patches-privilege-escalation-flaw-in-endpoint-client/
https://safebreach.com/Post/Check-Point-Endpoint-Security-Initial-Client-for-Windows-Privilege-Escalation-to-SYSTEM

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

Identifikátor

Trend Micro Password Manager zraniteľnosti

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Password Manager, ktorá opravuje bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

14.08.2019

CVE

CVE-2019-14684, CVE-2019-14687

Zasiahnuté systémy

Trend Micro Password Manager verzie staršie ako 5.0.0.1058

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://esupport.trendmicro.com/en-us/home/pages/technical-support/1123396.aspx
https://nvd.nist.gov/vuln/detail/CVE-2019-14684
https://safebreach.com/Post/Trend-Micro-Password-Manager-Privilege-Escalation-to-SYSTEM

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

Identifikátor

Kea zraniteľnosti

Popis

Vývojári DHCP servera Kea vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

28.08.2019

CVE

CVE-2019-6472, CVE-2019-6473, CVE-2019-6474

Zasiahnuté systémy

Kea verzie staršie ako 1.6.0, 1.5.0-P1 a 1.4.0-P2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2019/q3/181
https://exchange.xforce.ibmcloud.com/vulnerabilities/166131
https://exchange.xforce.ibmcloud.com/vulnerabilities/166132
https://exchange.xforce.ibmcloud.com/vulnerabilities/166133