BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 10. 2019 - 05. 11. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Zucchetti InfoBusiness zraniteľnosti	Vysoká	**8.8**
02.	ClipSoft REXPERT zraniteľnosti	Vysoká	**8.8**
03.	Phoenix Contact FL NAT zraniteľnosť	Vysoká	**8.2**
04.	Siemens produkty viacero zraniteľností	Vysoká	**7.9**
05.	OpenAFS zraniteľnosti	Vysoká	**7.5**
06.	European Commission eIDAS-Node zraniteľnosti	Vysoká	**7.5**

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/SK-CERT-261

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

Identifikátor

Zucchetti InfoBusiness zraniteľnosti

Popis

Spoločnosť Zucchetti vydala bezpečnostnú aktualizáciu na svoj produkt InfoBusiness, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.10.2019

CVE

CVE-2019-18204, CVE-2019-18205, CVE-2019-18206, CVE-2019-18207

Zasiahnuté systémy

Zucchetti InfoBusiness 4.4.1 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://blog.hacktivesecurity.com/index.php?controller=post&action=view&id_post=42
https://nvd.nist.gov/vuln/detail/CVE-2019-18205
https://nvd.nist.gov/vuln/detail/CVE-2019-18206
https://nvd.nist.gov/vuln/detail/CVE-2019-18207
https://nvd.nist.gov/vuln/detail/CVE-2019-18204

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

Identifikátor

ClipSoft REXPERT zraniteľnosti

Popis

Vývojári ClipSoft REXPERT vydali aktualizáciu svojho produktu, ktorá rieši bezpečnostné zraniteľnosti. Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených XML súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.10.2019

CVE

CVE-2019-17321, CVE-2019-17322, CVE-2019-17323, CVE-2019-17324, CVE-2019-17325, CVE-2019-17326

Zasiahnuté systémy

ClipSoft REXPERT verzie staršie ako 2.3.1

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://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35184
https://nvd.nist.gov/vuln/detail/CVE-2019-17321
https://nvd.nist.gov/vuln/detail/CVE-2019-17322
https://nvd.nist.gov/vuln/detail/CVE-2019-17323
https://nvd.nist.gov/vuln/detail/CVE-2019-17326
https://nvd.nist.gov/vuln/detail/CVE-2019-17325
https://nvd.nist.gov/vuln/detail/CVE-2019-17324

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

Identifikátor

Phoenix Contact FL NAT zraniteľnosť

Popis

Spoločnosť Phoenix Contact informovala o zraniteľnosti vo svojich FL NAT zariadeniach.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

29.10.2019

CVE

CVE-2019-18352

Zasiahnuté systémy

Phoenix Contact FL NAT 2208 a FL NAT 2304-2GC-2SFP

Následky

Neoprávnený prístup do systému

Odporúčania

Výrobca doposiaľ nevydal aktualizáciu riešiacu uvedenú zraniteľnosti. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://cert.vde.com/en-us/advisories/vde-2019-020

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens produkty viacero zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených UDP a TCP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

08.10.2019

CVE

CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-3615, CVE-2018-3620, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646, CVE-2019-10923, CVE-2019-10936, CVE-2019-11091, CVE-2019-13921, CVE-2019-13929

Zasiahnuté systémy

SIMATIC WinAC RTX 2010 verzie staršie ako SP3
SIMATIC IT UADM verzie staršie ako 1.3

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://cert-portal.siemens.com/productcert/txt/ssa-349422.txt
https://cert-portal.siemens.com/productcert/txt/ssa-473245.txt
https://cert-portal.siemens.com/productcert/txt/ssa-878278.txt
https://cert-portal.siemens.com/productcert/txt/ssa-984700.txt
https://cert-portal.siemens.com/productcert/txt/ssa-608355.txt
https://www.us-cert.gov/ics/advisories/icsa-19-281-04
https://www.us-cert.gov/ics/advisories/icsa-19-281-03

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

Identifikátor

OpenAFS zraniteľnosti

Popis

Vývojári systému OpenAFS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.10.2019

CVE

CVE-2019-18601, CVE-2019-18602, CVE-2019-18603

Zasiahnuté systémy

OpenAFS verzie staršie ako 1.6.24 a 1.8.5

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://openafs.org/pages/security/OPENAFS-SA-2019-001.txt
https://openafs.org/pages/security/OPENAFS-SA-2019-002.txt
https://openafs.org/pages/security/OPENAFS-SA-2019-003.txt
https://nvd.nist.gov/vuln/detail/CVE-2019-18602
https://nvd.nist.gov/vuln/detail/CVE-2019-18601
https://nvd.nist.gov/vuln/detail/CVE-2019-18603

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

Identifikátor

European Commission eIDAS-Node zraniteľnosti

Popis

Vývojári European Commission eIDAS-Node vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov pri overovaní certifikátov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

29.10.2019

CVE

CVE-2019-18632, CVE-2019-18633

Zasiahnuté systémy

European Commission eIDAS-Node verzie staršie ako 2.3.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, 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://sec-consult.com/en/blog/advisories/15587/
https://nvd.nist.gov/vuln/detail/CVE-2019-18633
https://nvd.nist.gov/vuln/detail/CVE-2019-18632