BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 01. 2018 – 16. 01. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Skóre
1	Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers Vulnerability	Vysoká	**8.6**
2	Oracle Fusion Middleware Vulnerability	Vysoká	**7.5**
3	IBM Security Access Manager Multiple Vulnerabilities	Vysoká	**7.4**
4	Adobe Flash Player Out-of-bounds Read	Vysoká	**7.1**
5	Multiple Vulnerabilities in SAP	Stredná	**6.5**
6	Sophos XG Web Application Firewall Cross-Site Scripting Vulnerability	Stredná	**6.1**
7	XSS in IBM WebSphere Portal	Stredná	**6.1**
8	Multiple vulnerabilities in Symantec ASG and ProxySG	Stredná	**5.6**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
00099/2018/SKB/OBPr-047

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Rockwell Automation Allen-Bradley MicroLogix 1400 Controllers Vulnerability

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Allen-Bradley MicroLogix 1400 Controllers, ktorá odstraňuje bezpečnostnú zraniteľnosť vo firmvéri uvedeného zariadenia. Vzdialený útočník by mohol využitím bezpečnostnej zraniteľnosti spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód alebo spôsobiť odopretie služieb na danom zariadení.

Dátum prvého zverejnenia varovania

09.01.2018 (posledná aktualizácia 11.01.2018)

CVE

CVE-2017-16740

Zasiahnuté systémy

Allen-Bradley MicroLogix 1400 Controllers

Následky

Vykonanie škodlivého kódu, Odopretie služieb

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizácie firmvéru uvedeného produktu a tiež zabezpečiť ochranu citlivých zariadení firewallovými riešeniami a obmedzením sieťového prístupu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-009-01

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

Identifikátor

Oracle Fusion Middleware Vulnerability

Popis

Komponent WebLogic Server produktu Oracle Fusion Middleware obsahuje kritickú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie ľubovoľného kódu. Zraniteľnosť spočíva v nesprávnej kontrole používateľských vstupov komponentom WebLogic Server a možno ju zneužiť odoslaním HTTP požiadavky so špecifickým formátom. Pre uvedenú zraniteľnosť je voľne dostupný exploit, ktorý zraniteľný systém infikuje softwarom na ťaženie kryptomeny.

Dátum prvého zverejnenia varovania

12.01.2018

CVE

CVE-2017-10271

Zasiahnuté systémy

Oracle Fusion Middleware 10.3 (.6.0.0)
Oracle Fusion Middleware 12.1 (.3.0)
Oracle Fusion Middleware 12.2 (.1.1, .1.2)

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých softwarov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56454

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

IBM Security Access Manager Multiple Vulnerabilities

Popis

Produkt IBM Security Access Manager obsahuje viacero zraniteľností. Najzávažnejšiu zraniteľnosť, ktorá spočíva v nesprávnom parsovaní URL odkazov, by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie phishing-ového útoku s cieľom získania citlivých údajov potrebných na prípravu ďalších útokov.

Dátum prvého zverejnenia varovania

05.01.2018 (posledná aktualizácia 12.01.2018)

CVE

CVE-2017-1534, CVE-2017-1459, CVE-2017-1478, CVE-2017-1533

Zasiahnuté systémy

IBM Security Access Manager appliances 9.0-9.0.3.0
IBM Security Access Manager for Mobile 8.0-8.0.1.6
IBM Security Access Manager for Web 8.0-8.0.1.6

Následky

Prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých produktov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56461
https://exchange.xforce.ibmcloud.com/vulnerabilities/130676

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Adobe Flash Player Out-of-bounds Read

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Adobe Flash Player. Uvedený produkt obsahuje bezpečnostnú zraniteľnosť známu ako Out-of-bounds Read, ktorú by vzdialený útočník mohol zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

09.01.2018

CVE

CVE-2018-4871

Zasiahnuté systémy

Adobe Flash Player verzia 28.0.0.126 a staršie

Následky

Prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom zasiahnutých produktov odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb18-01.html

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

Identifikátor

Multiple Vulnerabilities in SAP

Popis

V produktoch SAP Startup Service a SAP KERNEL pri volaní funkcií pre prácu s úložiskom nedochádza k autentifikácii používateľa. Uvedenú zraniteľnosť by útočník mohol zneužiť na zahltenie systémového úložiska.
V produkte SAP Solution Manager je nesprávne nastavený parameter *SAP_BPO_CONFIG*, ktorý BPO (Business Process Operations) používateľovi dáva právomoci aj nad rámec štandardnej konfigurácie BPO nástrojov.
Produkt SAP HANA obsahuje zraniteľnosť, ktorú by vzdialený útočník prostredníctvom špeciálnej SOAP požiadavky smerovanej na SAP Startup Service mohol zneužiť na prístup k citlivým údajom.
Produkty SAP NetWeaver a SAP BASIS obsahujú zraniteľnosť umožňujúcu vykonanie ľubovoľného používateľom zadaného kódu. Uvedenú zraniteľnosť by útočník mohol zneužiť na získanie kontroly nad systémom.

Dátum prvého zverejnenia varovania

09.01.2018

CVE

CVE-2018-2360, CVE-2018-2361, CVE-2018-2362, CVE-2018-2363

Zasiahnuté systémy

SAP Startup Service, SAP KERNEL 7.45, 7.49 a 7.52
SAP Solution Manager 7.20
SAP HANA 1.00 a 2.00
SAP NetWeaver, SAP BASIS verzie 7.00 až 7.02, 7.10 až 7.11, 7.30, 7.31, 7.40, 7.50 až 7.52

Následky

Prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Spoločnosť SAP vydala aktualizácie, ktoré riešia uvedené zraniteľnosti. Administrátorom dotknutých systémov odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://blogs.sap.com/2018/01/09/sap-security-patch-day-january-2018/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Sophos XG Web Application Firewall Cross-Site Scripting Vulnerability

Popis

Komponent Application Firewall produktu Sophos XG Firewall Operating System obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie XSS útoku. Cieľom je prinútiť používateľa, aby navštívil stránku zobrazujúcu záznamy WAF obsahujúcu škodlivý skript, ktorý útočníkovi umožní vykonávať operácie v kontexte *webadmin*. Zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov.

Dátum prvého zverejnenia varovania

03.01.2018

CVE

CVE-2017-18014

Zasiahnuté systémy

SFOS verzie 15, 16 a 17

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizácie uvedeného produktu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56439s
http://seclists.org/fulldisclosure/2018/Jan/24

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

XSS in IBM WebSphere Portal

Popis

Produkt IBM WebSphere Portal obsahuje bezpečnostnú zraniteľnosť, ktorá umožňuje vykonanie XSS (Cross-Site Scripting) útoku. Vložením JavaScript-ového kódu do Web UI rozhrania by vzdialený útočník mohol zraniteľnosť zneužiť na získanie prístupu k citlivým údajom (prihlasovacie údaje).

Dátum prvého zverejnenia varovania

09.01.2018

CVE

CVE-2018-1361

Zasiahnuté systémy

IBM WebSphere Portal 9.0.0.0 - 9.0.0.0 CF15
IBM WebSphere Portal 8.5.0.0 - 8.5.0.0 CF15

Následky

Prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu uvedených produktov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22012409

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.6**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Multiple vulnerabilities in Symantec ASG and ProxySG

Popis

Manažmentové konzoly produktov Symantec ASG a ProxySG obsahujú viacero zraniteľností, ktoré by vzdialený útočník mohol zneužiť na získanie autentifikačných údajov, presmerovanie používateľov na stránky so škodlivým obsahom alebo injekciu ľubovoľného JavaScript-ového kódu do konzol.

Dátum prvého zverejnenia varovania

09.01.2018

CVE

CVE-2016-9099, CVE-2016-9100, CVE-2016-10256, CVE-2016-10257

Zasiahnuté systémy

Advanced Secure Gateway verzie 6.6 a 6.7
ProxySG verzie 6.5, 6.6 a 6.7

Následky

Prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu, ktorá odstraňuje uvedené zraniteľnosti dotknutých produktov.

Zdroje

https://www.symantec.com/security-center/network-protection-security-advisories/SA155