BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 12. 2017 – 19. 12. 2017

OBSAH BEZPEČNOSTNÉHO BULLETINU

Číslo	Identifikátor	Dôležitosť	CVSS Score
1	Progress Telerik UI RadAsyncUpload User Input Vulnerability	Kritická	9.1
2	Stable Chanel update for Google Chrome	Vysoká	8.8
3	Palo Alto Networks PAN-OS Vulnerabilities	Vysoká	8.8
4	Microsoft Internet Explorer Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System	Vysoká	7.5
5	XMLSoft libxml2 multiple issues	Vysoká	7.5
6	Multiple vulnerabilities fixed in SAP product portfolio	Vysoká	7.3
7	Apple Releases Security Updates	Vysoká	7.3
8	TLS implementations may disclose side channel information via discrepencies between valid and invalid PKCS#1 padding	Vysoká	7.1
9	GNU glibc Memory Leak and Buffer Overflow Vulnerability	Vysoká	7.0
10	KRACK Attacks Vulnerabilities in SIEMENS SIMATIC RF350M and SIMATIC RF650M	Stredná	6.8
11	IBM WebSphere Portal Web Application Bridge Information Disclosure Vulnerability	Stredná	5.3

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:
06282/2017/SKB/OBPr-036

BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 12. 2017 – 19. 12. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.1**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Progress Telerik UI RadAsyncUpload User Input Vulnerability

Popis

Zraniteľnosť v Progress Telerik UI pre ASP.NET AJAX umožňuje vzdialenému útočníkovi vykonať škodlivý kód. Zraniteľnosť spočíva v nedostatočnom overovaní vstupných hodnôt používateľa vo funkcii RadAsyncUpload.

Dátum prvého zverejnenia varovania

14.12.2017

CVE

CVE-2017-11357

Zasiahnuté systémy

Progress Telerik UI for ASP.NET AJAX

Následky

Neoprávnené vykonanie kódu

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56270

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

Identifikátor

Stable Chanel update for Google Chrome

Popis

Spoločnosť Google vydala aktualizáciu na produkt Google Chrome, verzia 63.0.3239.108, ktorá obsahuje opravu bezpečnostnej zraniteľnosti v komponente V8. Vzdialený útočník môže pomocou podvrhnutého webového obsahu spôsobiť pád aplikácie a neoprávnené vykonanie kódu.

Dátum prvého zverejnenia varovania

14.12.2017

CVE

CVE-2017-15429

Zasiahnuté systémy

Google Chrome

Následky

Neoprávnené vykonanie kódu, Neprístupnosť služby, Únik citlivých informácií

Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

Zdroje

https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop_14.html
https://access.redhat.com/security/cve/cve-2017-15429

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

Identifikátor

Palo Alto Networks PAN-OS Vulnerabilities

Popis

Bezpečnostné zraniteľnosti v Palo Alto Networks PAN-OS umožňujú vzdialenému útočníkovi vykonať škodlivý kód a spôsobiť odopretie služby. Zraniteľnosti sa nachádzajú v používateľskom rozhraní, pričom útočník môže vďaka nedostatočnému overovaniu vstupov vykonávať škodlivé príkazy a zaslaním špecifickej požiadavky spôsobiť nedostupnosť používateľského rozhrania dotknutého zariadenia.

Dátum prvého zverejnenia varovania

13.12.2017

CVE

CVE-2017-15940, CVE-2017-15942, CVE-2017-15943, CVE-2017-15944

Zasiahnuté systémy

Palo Alto Networks PAN-OS 6.1, 7.0, 7.1, 8.0

Následky

Neoprávnená zmena v systéme, Vykonanie škodlivého kódu, Odopretie služby, Únik citlivých informácií

Odporúčania

Administrátorom uvedených produktov odporúčame vykonať bezpečnostnú aktualizáciu.

Zdroje

https://securityadvisories.paloaltonetworks.com/Home/Detail/105
https://securityadvisories.paloaltonetworks.com/Home/Detail/102
https://securityadvisories.paloaltonetworks.com/Home/Detail/99
https://securityadvisories.paloaltonetworks.com/Home/Detail/96
https://tools.cisco.com/security/center/viewAlert.x?alertId=56242
https://tools.cisco.com/security/center/viewAlert.x?alertId=56239

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

Identifikátor

Microsoft Internet Explorer Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System

Popis

Viacero bezpečnostných zraniteľností v internetovom prehliadači Microsoft Internet Explorer umožňuje vzdialenému útočníkovi získať citlivé informácie. Vzdialený útočník môže pomocou podvrhnutého webového obsahu spôsobiť chyby vo vnútornej pamäti, ktoré môžu viesť k úniku citlivých informácií a eskalácií privilégií.

Dátum prvého zverejnenia varovania

12.12.2017 (posledná aktualizácia 13.12.2017)

CVE

CVE-2017-11887, CVE-2017-11901, CVE-2017-11906, CVE-2017-11907, CVE-2017-11919

Zasiahnuté systémy

Microsoft Internet Explorer 9; 10; 11

Následky

Únik citlivých informácií, Eskalácia privilégií

Odporúčania

Administrátorom a používateľom dotknutých softvérov odporúčame vykonať aktualizáciu.

Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11887
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11906
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11907
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11919
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11901
https://www.securitytracker.com/id/1039993

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

Identifikátor

XMLSoft libxml2 multiple issues

Popis

Bezpečnostné zraniteľnosti vo viacerých funkciách v XMLSoft libxml2 umožňujú vzdialenému útočníkovi spôsobiť odopretie služieb.
Vzdialený útočník môže prostredníctvom podvrhnutých škodlivých súborov a požiadaviek spôsobiť pretečenie zásobníka a následné odopretie služieb.

Dátum prvého zverejnenia varovania

13.12.2017

CVE

CVE-2017-8872, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Zasiahnuté systémy

Libxml2 2.9

Následky

Neprístupnosť služby

Odporúčania

Administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

Zdroje

http://www.vuxml.org/freebsd/76e59f55-4f7a-4887-bcb0-11604004163a.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=56257
https://tools.cisco.com/security/center/viewAlert.x?alertId=56253
https://tools.cisco.com/security/center/viewAlert.x?alertId=56254

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Multiple vulnerabilities fixed in SAP product portfolio

Popis

Viacero produktov spoločnosti SAP obsahuje bezpečnostné zraniteľnosti:
V SAP NetWeaver Knowledge Management Configuration Service útočník môže vykonať SSRF útok.
V rámci SAP Startup Service útočník môže presmerovať používateľa na stránku so škodlivým obsahom.
V SAP HANA nedochádza k správnemu overovaniu používateľských vstupov v niektorých HTTP/REST koncových bodoch a pri zápise do syslog-u pri procese overovania používateľov, čo útočníkovi umožňuje do audit log-u injektovať záznamy.
V SAP Business Intelligence Promotion Management Application nedochádza k autentifikácii vo funkciách viazaných na identitu používateľa a útočník môže vykonať XSS útok.
SAP ITS útočníkovi s admin prístupom do aplikácie vložiť kusy kódu a ovplyvniť tak jej správanie.
V SAP Business Objects Platform by útočník prostredníctvom DOS útoku mohol spôsobiť neprístupnosť služby.

Dátum prvého zverejnenia varovania

12.12.2017 (posledná aktualizácia 15.12.2017)

CVE

CVE-2017-16678, CVE-2017-16679, CVE-2017-16680, CVE-2017-16681, CVE-2017-16682, CVE-2017-16683, CVE-2017-16684, CVE-2017-16685, CVE-2017-16687, CVE-2017-16690, CVE-2017-16691

Zasiahnuté systémy

SAP NetWeaver Knowledge Management Configuration Service, EPBC a EPBC2 od v. 7.00-7.02; KMC-BC v. 7.30, 7.31, 7.40 a 7.50
SAP's Startup Service, SAP KERNEL 32 NUC, SAP KERNEL 32 Unicode, SAP KERNEL 64 NUC, SAP KERNEL 64 Unicode 7.21, 7.21EXT, 7.22 a 7.22EXT; SAP KERNEL 7.21, 7.22, 7.45, 7.49 and 7.52
SAP HANA, SAP HANA Database versions 1.00 and 2.00
SAP Business Intelligence Promotion Management Application, Enterprise 4.10, 4.20, 4.30
SAP NetWeaver Internet Transaction Server (ITS), SAP Basis from 7.00 to 7.02, 7.30, 7.31, 7.40, from 7.50 to 7.52, SAP Business Objects Platform, Enterprise 4.10 and 4.20
SAP Business Warehouse Universal Data Integration, from 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50

Následky

Neprístupnosť služby, Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom dotknutých softvérov odporúčame bezodkladne vykonať aktualizáciu.

Zdroje

https://blogs.sap.com/2017/12/12/sap-security-patch-day-december-2017/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Apple Releases Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty iOS 11.2.1, tvOS 11.2.1, iCloud for Windows 7.2, ktoré obsahujú viacero zraniteľností.
Zneužitím uvedených zraniteľností by vzdialený útočník mohol obísť zabezpečenie uvedených produktov, ovplyvniť beh aplikácií a získať prístup do systému.

Dátum prvého zverejnenia varovania

13.12.2017

CVE

CVE-2017-13903, CVE-2017-13864, CVE-2017-7156, CVE-2017-7157, CVE-2017-13856, CVE-2017-13870, CVE-2017-13866

Zasiahnuté systémy

iOS 11, 11.1, 11.2; tvOS 11, 11.1, 11,2; iCloud for Windows 7.2.

Následky

Neoprávnený prístup do systému

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať štandardnú aktualizáciu zasiahnutých produktov.

Zdroje

https://support.apple.com/en-in/HT208357
https://support.apple.com/en-in/HT208359
https://support.apple.com/en-us/HT208328

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

Identifikátor

TLS implementations may disclose side channel information via discrepencies between valid and invalid PKCS#1 padding

Popis

Zistená zraniteľnosť v TLS serveroch umožňuje vzdialenému útočníkovi na základe informácií z chybových správ zraniteľných TLS serverov dešifrovať RSA (TLS_RSA) šifrovanú komunikáciu a podpisovať komunikáciu privátnym kľúčom TLS servera.

Dátum prvého zverejnenia varovania

08.12.2017, aktualizované 14.12.2017

CVE

CVE-2017-6168, CVE-2017-1000385, CVE-2017-17427, CVE-2017-13098, CVE-2017-13099, CVE-2017-17428, CVE-2017-17382

Zasiahnuté systémy

F5; Citrix; Radware; Cisco ACE; Cisco ASA; Bouncy Castle; Erlang; WolfSSL

Následky

Únik citlivých informácií

Odporúčania

Administrátorom odporúčame vypnúť RSA šifrovací algoritmus (TLS_RSA) na TLS serveroch. Následne odporúčame vykonať štandardnú aktualizáciu uvedených produktov.

Zdroje

https://robotattack.org/
http://www.kb.cert.org/vuls/id/144389

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

GNU glibc Memory Leak and Buffer Overflow Vulnerability

Popis

Bezpečnostná zraniteľnosť v dynamic loader (*ld.so*) v GNU knižnici *glibc* umožňuje *vzdialenému útočníkovi prostredníctvom podvrhnutých hodnôt LD_LIBRARY_PATH spôsobiť pretečenie zásobníka a následné odopretie služieb.*

Dátum prvého zverejnenia varovania

11.12.2017

CVE

CVE-2017-1000408, CVE-2017-1000409

Zasiahnuté systémy

GNU Glibc

Následky

Odopretie služieb

Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

Zdroje

https://sourceware.org/git/gitweb.cgi?p=glibc.git;a=patch;h=efa26d9c13a6fabd34a05139e1d8b2e441b2fae9
http://seclists.org/oss-sec/2017/q4/385
https://tools.cisco.com/security/center/viewAlert.x?alertId=56244

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

Identifikátor

KRACK Attacks Vulnerabilities in SIEMENS SIMATIC RF350M and SIMATIC RF650M

Popis

Zasiahnuté produkty spoločnosti SIEMENS obsahujú viacero zraniteľností v implementácii WPA/WPA2, ktoré možno zaradiť do skupiny "Key Reinstallation Arrack" (KRACK).
Bezpečnostné zraniteľnosti by útočník v dosahu bezdrôtovej siete mohol zneužiť na dešifrovanie, opakované zaslanie alebo vkladanie vlastných paketov do prebiehajúcej bezdrôtovej komunikácie.

Dátum prvého zverejnenia varovania

18.12.2017

CVE

CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081

Zasiahnuté systémy

SIMATIC RF350M: všetky verzie s Summit Client Utility < V22.3.5.16
SIMATIC RF650M: všetky verzie s Summit Client Utility < V22.3.5.16

Následky

Únik citlivých informácií

Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

Zdroje

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-418456.pdf

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.3**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

IBM WebSphere Portal Web Application Bridge Information Disclosure Vulnerability

Popis

Spoločnosť IBM vydala aktualizáciu na produkt IBM WebSphere Portal, ktorá obsahuje opravu bezpečnostnej zraniteľnosti v komponente Web Application Bridge. Vzdialený útočník môže vďaka expozícii backend URL adries získať citlivé informácie.

Dátum prvého zverejnenia varovania

15.12.2017

CVE

CVE-2017-1423

Zasiahnuté systémy

IBM WebSphere Portal 8.5; 9.0

Následky

Únik citlivých informácií

Odporúčania

Administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22011400
https://tools.cisco.com/security/center/viewAlert.x?alertId=56285