BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 11. 2017 – 05. 12. 2017

OBSAH BEZPEČNOSTNÉHO BULLETINU

BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 11. 2017 – 05. 12. 2017

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

Identifikátor

Multiple vulnerabilities in Thunderbird

Popis

Poštový klient Thunderbird obsahuje viacero bezpečostných zraniteľností. Útočník by otvorením webových stránok so špecifickým obsahom mohol obísť obmedzenie politiky rovnakého pôvodu (same-origin), vyvolať pád aplikácie, spôsobiť nedostupnosť služby alebo vykonať škodlivý kód.

Same-origin je dôležitý koncept v modeli bezpečnosti webových aplikácií. Podľa same-origin pravidiel webový prehliadač umožňuje skriptom obsiahnutým na prvej webovej stránke prístup k údajom na druhej webovej stránke, ale iba v prípade, že obe webové stránky majú rovnaký pôvod. Tieto pravidlá zabraňujú tomu, aby škodlivý skript na jednej stránke získal prístup k citlivým údajom na inej webovej stránke prostredníctvom Document Object Model tejto stránky.

Dátum prvého zverejnenia varovania

01.12.2017

CVE

CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Zasiahnuté systémy

Ubuntu 17.10, Ubuntu 17.04, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS

Následky

Neoprávnené vykonanie kódu, Nedostupnosť služby

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutých operačných systémov a buildov softvéru Thunderbird:

Ubuntu 17.10: thunderbird 1:52.5.0+build1-0ubuntu0.17.10.1
Ubuntu 17.04: thunderbird 1:52.5.0+build1-0ubuntu0.17.04.1
Ubuntu 16.04 LTS: thunderbird 1:52.5.0+build1-0ubuntu0.16.04.1
Ubuntu 14.04 LTS: thunderbird 1:52.5.0+build1-0ubuntu0.14.04.1

Zdroje

https://usn.ubuntu.com/usn/usn-3490-1/
https://access.redhat.com/errata/RHSA-2017:3372

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

Identifikátor

Ubuntu Security Notice USN-3496-1, USN-3496-2, USN-3496-3:Python vulnerability

Popis

Nižšie uvedené verzie vysokoúrovňového objektovo-orientovaného jazyka Python obsahujú bezpečnostnú zraniteľnosť. CPython (Python) je zraniteľný voči integer overflow vo funkcii PyString_DecodeEscape v stringobject.c, ktoré vedie k pretečeniu zásobníka dynamickej pamäte. Útočník by uvedenú zraniteľnosť mohol využiť na neoprávnené vykonanie kódu.

Dátum prvého zverejnenia varovania

28.11.2017

CVE

CVE-2017-16613

Zasiahnuté systémy

python2.7 (Ubuntu 17.04, Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 12.04 ESM), python3.4, python3.5 (Ubuntu 17.04, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS)

Následky

Neoprávnené vykonanie kódu

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať štandardnú aktualizáciu zasiahnutých operačných systémov.

Zdroje

www.linuxsecurity.com/content/view/198293?rdf
www.linuxsecurity.com/content/view/198298?rdf
http://www.linuxsecurity.com/content/view/198306?rdf

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

Identifikátor

Apache Struts Jackson Databind Deserialization Code Execution Vulnerability

Popis

Zraniteľnosti v Apache Struts môžu umožniť vzdialenému útočníkovi spustenie škodlivého kódu.
Zraniteľnosť sa nachádza v ObjectMapper vo funkcii readValue() a spočíva v nedostatočnej kontrole vstupných hodnôt v dotknutom softvéri. Útočník môže pomocou súboru so špecifickým obsahom spôsobiť chybu a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

04.12.2017

CVE

CVE-2017-7525, CVE-2017-15707

Zasiahnuté systémy

Apache Struts 2.5 (.0, .1, .2, .5, .8, .10, .10.1, .12, .14)

Následky

Vykonanie škodlivého kódu, odopretie služby

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu dotknutého softvéru.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56117
https://tools.cisco.com/security/center/viewAlert.x?alertId=56116
https://cwiki.apache.org//confluence/display/WW/S2-055
https://cwiki.apache.org//confluence/display/WW/S2-054

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

Identifikátor

Procmail loadbuf Function Heap Buffer Overflow Vulnerability

Popis

Bezpečnostná zraniteľnosť loadbuf funkcie v Procmail umožňuje útočníkovi so vzdialeným prístupom spustiť škodlivý kód a spôsobiť odopretie služieb (DoS).
Zraniteľnosť je spôsobená nesprávnym spracovaním emailových správ dotknutým softvérom. Útočník môže pomocou podvrhnutej emailovej správy spôsobiť pretečenie zásobníka v dôsledku pevne určenej prerozdeľovacej veľkosti vo funkcii loadbuf v súbore formail formisc.c danej aplikácie.

Dátum prvého zverejnenia varovania

28.11.2017 (posledná aktualizácia 29.11.2017)

CVE

CVE-2017-16844

Zasiahnuté systémy

Procmail 3.22

Následky

Neoprávnené vykonanie škodlivého kódu, odopretie služby

Odporúčania

Administrátorom odporúčame aktualizovať procmail balík.

Zdroje

https://packetstormsecurity.com/files/145140/RHSA-2017-3269-01.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=56007

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

Identifikátor

Multiple curl vulnerabilities

Popis

libcurl v autentifikačnom kóde NTLM na 32-bitových platformách obsahuje zraniteľnosť založenú na pretečení zásobníka.Útočník by pretečenie zásobníka mohol využiť na spôsobenie pádu aplikácie a k zneprístupneniu služby.
libcurl vo funkcii zodpovednej za spracovanie FTP wildcard obsahuje zraniteľnosť umožňujúcu out-of-bounds čítanie. Vzdialený útočník by zraniteľnosť mohol zneužiť na spôsobenie pádu aplikácie a teda zneprístupnenie služby a môže spôsobiť aj únik citlivých informácií.
libcurl obsahuje zraniteľnosť, kde pre interface s knižnicou SSL nedochádza k alokácii dostatočne veľkej pamäte. Útočník by zraniteľnosť mohol využiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.11.2017

CVE

CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Zasiahnuté systémy

curl, libcurl verzie pred 7.57.0

Následky

Neprístupnosť služby

Odporúčania

Predmetné zraniteľnosti možno opraviť aktualizáciou operačného systému: Ubuntu 17.10, Ubuntu 17.04, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS.

Zdroje

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8816
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8817
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-8818

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

Identifikátor

Mozilla Releases Security Updates

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu, ktorá rieši viacero zraniteľností v produktoch Firefox 57. Zneužitím týchto zraniteľností by útočník mohol zistiť, ktoré stránky používateľ v minulosti navštívil alebo získať identitu používateľa napriek použitiu private browsing mode.

Dátum prvého zverejnenia varovania

04.12.2017

CVE

CVE-2017-7843, CVE-2017-7844

Zasiahnuté systémy

Mozilla Firefox starší ako verzia 57.0.1.

Následky

Neprístupnosť služby

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu vyššie uvedeného zraniteľného softvéru.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-27/

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

Identifikátor

Multiple vulnerabilities in Wordpress CMS

Popis

Skript wp-admin/user-new.php nastavuje kľúč nového používateľa na hodnotu, ktorú možno priamo odvodiť z ID používateľa. Vzdialený útočník by mohol zadaním tejto hodnoty získať neoprávnený prístup do systému.
Skript wp-includes/functions.php umožňuje používateľom bez unfiltered_html uploadovať JavaScript súbory. Vzdialený útočník by prostredníctvom špecificky vytvoreného súboru mohol vykonať XSS útoky.
Skript wp-includes/general-template.php nesprávne ošetruje jazykové obmedzenia obsahu HTML elementov. Útočník by zraniteľnosť mohol využiť na realizáciu XSS útokov.
Skript wp-includes/feed.php nesprávne ošetruje obsah pridávaný do RSS a Atom feedov. Útočník by prostredníctvom URL so špecifickým obsahom vedel vykonať XSS útoky.

Dátum prvého zverejnenia varovania

02.12.2017

CVE

CVE-2017-17091, CVE-2017-17092, CVE-2017-17093, CVE-2017-17094

Zasiahnuté systémy

CMS Wordpress pred verziou 4.9.1

Následky

Neoprávnený prístup do systému, XSS útok

Odporúčania

Používateľom a administrátorom redakčného systému Wordpress odporúčame vykonať aktualizáciu na verziu 4.9.1 a udržiavať systém aktualizovaný

Zdroje

https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/