SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-01V

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

Identifikátor

SK-CERT Phyton advisory

Popis

SK-CERT identifikoval knižnice so škodlivým softvérom v oficiálnom balíku Pythonu, PyPI, ktoré predstavujú oficiálne knižnice. Významným príkladom je falošný balíček urllib-1.21.1.tar.gz na základe oficiálneho balíka urllib3-1.21.1.tar.gz.
Takéto balíky mohli byť prevzaté nevedomým vývojárom alebo správcom rôznymi prostriedkami vrátane populárnej utility "pip" (pip install urllib). Existujú dôkazy, že falšované balíky boli skutočne stiahnuté a začlenené do softvéru niekoľkokrát medzi júnom 2017 a septembrom 2017.

Dátum prvého zverejnenia varovania

14. 09. 2017

SK-CERT Advisory ID

skcsirt-sa-20170909-pypi-malicious-code

Zasiahnuté systémy

Python všetky verzie OS zahrňujúce Windows, Linux a Mac OS

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Všetky odporúčania nájdete na:
http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/index.html

Zdroje

http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/index.html

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-004

SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-02V

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

Identifikátor

VMware Security Advisories

Popis

Spoločnosť VMware vydala niekoľko aktualizácií svojich softvérových produktov, u ktorých boli zistené závažné zraniteľnosti:

1. Softvér VMware ESXi, Workstation a Fusion obsahujú zraniteľnosť pri zápisoch mimo zariadenia SVGA. Tento problém môže povoliť guestovi vykonať kód na hostovi.
2. Softvér VMware ESXi, Workstation a Fusion obsahujú zraniteľnosť dereferencie ukazovateľa NULL. K tomuto problému dochádza pri spracovávaní žiadostí RPC guesta. Úspešné zneužitie tohto problému môže útočníkom s bežnými používateľskými oprávneniami umožniť zhodenie ich VM.
3. Klient vCenter Server H5 obsahuje zraniteľnosť, ktorá môže umožniť cross side scripting (XSS). Útočník s oprávneniami používateľa VC môže vniesť škodlivé java-skripty, ktoré sa vykonajú, keď ostatní používatelia VC pristupujú na stránku.

Dátum prvého zverejnenia varovania

14. 09. 2017

CVE

CVE-2017-4924, CVE-2017-4925, CVE-2017-4926

Vendor ID (VMware advisory ID)

VMSA-2017-0015.1

Zasiahnuté systémy

VMware ESXi verzie 5.5, 6.0 a 6.5, VMware Workstation verzia 12.x, VMware Fusion verzia 8.x, vCenter Server H5 verzie 5.5, 6.0 a 6.5

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Spoločnosť VMware vydala bezplatné aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Odporúčame preto bezodkladnú aktualizáciu VMware produktov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2017-0015.html

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-004

SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-03V

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

Identifikátor

BlueBorne – pack of Bluetooth implementation vulnerabilities

Popis

Bol vydaný súbor viacerých zraniteľností Bluetooth implementácií, známych pod názvom „BlueBorne“.
Zraniteľnosť „BlueBorne“ neobchádza žiadne typy ani značky zariadení, táto zraniteľnosť postihuje všetky operačné systémy aj väčšinu výrobcov mobilných zariadení, zariadení „Internet of Things“ a ostatných produktov, ktoré využívajú technológiu Bluetooth. Pre využitie zraniteľnosti stačí mať zapnuté na zariadení Bluetooth.
Útočník, ktorý využije zraniteľnosť, zaradenú do súboru „BlueBorne“, môže prebrať celkovú kontrolu nad napadnutým zariadením a prostredníctvom tohto zariadenia vie šíriť škodlivý kód na ďalšie zariadenia a takisto sa môže cez napadnuté zariadenie dostať do zabezpečených sietí, ku ktorým má zariadenie prístup.

Dátum prvého zverejnenia varovania

14. 09. 2017

Technická analýza

Kompletnú technickú analýzu nájdete na:
http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf

CVE

CVE-2017-1000251, CVE-2017-1000250, CVE-2017-0785, CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-8628, CVE-2017-14315

Zasiahnuté systémy

Android OS, Apple, Google, Microsoft Corporation Samsung Mobile, Tizen

Následky

Neoprávnené vykonanie škodlivého kódu, neoprávnený prístup k informáciám a systémom

Odporúčania

Bezodkladne aplikujte aktualizácie vašich mobilných zariadení bez ohľadu na používaný operačný systém alebo výrobcu zariadenia. Aktualizácie boli vydané na operačné systémy Android, iOS, Linux, Microsoft OS.

Zdroje

https://www.kb.cert.org/vuls/id/240311
http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf

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-004

SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-04V

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

Identifikátor

Apache Struts 2 Remote code execution vulnerability

Popis

V Apache Struts 2 sa objavilo možné spustenie vzdialeného kódu prostredníctvom zraniteľnosti v doplnku REST za použitia XStream programu, ktorý spracováva XML dáta. Plugin REST používa XStreamHandler s inštanciou XStream na deserializáciu bez akéhokoľvek filtrovania typu a môže to viesť k vzdialenému vykonávaniu kódu pri deserializácii užitočných dát XML.

Dátum prvého zverejnenia varovania

06. 09. 2017

CVE

CVE-2017-9805

Vendor ID (Apache)

S2-052

Zasiahnuté systémy

Apache Struts 2.1.2 až Struts 2.3.33, Struts 2.5 až Struts 2.5.12

Následky

Neoprávnené vykonanie škodlivého kódu

Odporúčania

Spoločnosť Apache vydala aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie na verziu 2.5.13 alebo 2.3.34, podľa verzie vášho produktu.

Zdroje

https://cwiki.apache.org/confluence/display/WW/S2-052
https://www.kb.cert.org/vuls/id/112992

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-004

SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-05V

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

Identifikátor

Wordpress plugin Display Widgets backdoor code

Popis

V plugine Display Widgets, ktorý je možné inštalovať ako súčasť Content Managment Systému (CMS) Wordpress , bol objavený backdoor kód, ktorý zasielal citlivé informácie z webových stránok, ktoré mali tento plugin nainštalovaný, na server tretej strany.
Škodlivý kód sa do pluginu dostal priamo prostredníctvom autora pluginu, ktorý takýmto spôsobom zbieral informácie od zasiahnutých webových stránok a okrem toho backdoor využíval aj na pridávanie spamového obsahu na zasiahnuté webové stránky.
Spoločnosť Wordpress.org plugin stiahla z oficiálneho obchodu s pluginmi na CMS Wordpress. Zároveň upozornila, že tento plugin si stiahlo celkovo 200 000 používateľov.

Dátum prvého zverejnenia varovania

13. 09. 2017

Zasiahnuté systémy

Wordpress CMS

Následky

Neoprávnený prístup k citlivým informáciám, únik citlivých informácií, neoprávnené pridávanie obsahu

Odporúčania

Ak používate plugin Display Widgets na svojej webovej stránke, ktorá je založená na CMS Wordpress, odporúčame vám tento plugin bezodkladne odinštalovať a nájsť za tento plugin alternatívu, ak ide o plugin, ktorý je nutný na fungovanie vašej webovej stránky.

Zdroje

https://www.bleepingcomputer.com/news/security/backdoor-found-in-wordpress-plugin-with-more-than-200-000-installations/
https://www.wordfence.com/blog/2017/09/display-widgets-malware/
https://wptavern.com/display-widgets-plugin-permanently-removed-from-wordpress-org-due-to-malicious-code

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-004

SECURITY BULLETIN

Týždeň 12. 09. 2017 – 19. 09. 2017

No: B20170919-06V

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

Identifikátor

tcpdump vulnerabilities

Popis

Spoločnosť Ubuntu vydala upozornenie na niekoľko zraniteľností, ktoré zasahujú softvér tcpdump.
Ide o zraniteľnosti, ktoré umožňujú útočníkovi útok typu buffer overflow a DoS (zneprístupnenie služby).

Dátum prvého zverejnenia varovania

13. 09. 2017

CVE

Kompletný zoznam na:
https://usn.ubuntu.com/usn/usn-3415-1/

Vendor ID (Ubuntu Security Notice)

USN-3415-1

Zasiahnuté systémy

Ubuntu 17.04
Ubuntu 16.04 LTS
Ubuntu 14.04 LTS

Následky

Buffer overflow, zneprístupnenie služby

Odporúčania

Spoločnosť Ubuntu vydala aktualizácie softvéru, ktoré riešia predmetnú zraniteľnosť. Ak využívate tento produkt, bezodkladne aktualizujte svoje zariadenie.

Zdroje

https://usn.ubuntu.com/usn/usn-3415-1/