NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-01K

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

SBroadcom BCM43xx Wi-Fi chipset vulnerability „Broadpawn“

Popis

Ide o zraniteľnosť, ktorá je založená na chybe vo Wi-Fi chipsete rodiny Broadcom BCM43xx, ktorá sa využíva v mobilných zariadeniach, vystupujúca pod názvom „Broadpawn“. Ide o chybu, ktorá umožňuje útočníkovi spustiť ľubovoľný kód na zariadení bez interakcie používateľa tohto zariadenia. Nakoľko ide o chybu Wi-Fi chipsetu, útočník sa musí nachádzať v blízkosti zariadenia, na ktoré útočí.

CVE

CVE-2017-9417

Zasiahnuté systémy

Mobilné zariadenia (Apple iPhone, Samsung, HTC, Nexus, LG a mnoho ďalších) s Broadcom BCM43xx Wi-Fi chipsetom

Následky

Neoprávnený prístup k informáciám, Neoprávnená zmena informácií, Zneprístupnenie služby

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu operačného systému vašich mobilných zariadení, ktoré fungujú na platformách Android a iOS.

Apple vydal na iOS aktualizáciu 10.3.3, ktorá opravuje túto zraniteľnosť.

Podrobnosti o aktualizáciách a zraniteľnosti na iOS:
https://support.apple.com/en-us/HT207923

Podrobnosti o aktualizáciách a zraniteľnosti na Android:
https://source.android.com/security/bulletin/2017-07-01

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2017-9417
http://boosterok.com/blog/broadpwn/

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
Národná jednotka reakcie
na núdzové počítačové situácie

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-02V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Cross-site Request Forgery (CSRF) security vulnerability in IBM WebSphere Commerce

Popis

IBM WebSphere Commerce obsahuje zraniteľnosť voči cross-site request forgery (CSRF), spôsobená nesprávnym overením užívateľských vstupov. Po návšteve infikovanej webovej stránky používateľom môže útočník vyslať vzdialenú chybnú HTTP žiadosť. Následne môže útočník túto zraniteľnosť použiť na vykonávanie cross-site scripting útokov (XSS), infikovanie web cache a iných škodlivých aktivít.

CVE

CVE-2016-2863

Zasiahnuté systémy

WebSphere Commerce - verzie 8.0.1.0 – 8.0.1.1
WebSphere Commerce - verzie 8.0.0.0 – 8.0.0.9
WebSphere Commerce - verzie 7 Feature Pack 8

Následky

Neoprávnené spustenie škodlivého kódu

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu vašich WebSphere Commerce produktov

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg21983626

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
Národná jednotka reakcie
na núdzové počítačové situácie

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-03V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Samba vulnerability

Popis

Vo všetkých verziách implementácie Samby od 3.5.0 sa vyskytuje zraniteľnosť, ktorá umožňuje vykonať vzdialený kód, ktorý umožňuje útočníkovi nahrať zdieľanú knižnicu do zapisovateľnej zdieľanej zložky a následne ju načítať a spustiť.

CVE

CVE-2017-7494

Zasiahnuté systémy

Samba od verzie 3.5.0

Následky

Neoprávnené spustenie škodlivého kódu

Odporúčania

Odporúčame aktualizovať Sambu na verzie 4.6.4, 4.5.10 a 4.4.14, ak používate staršie verzie Samby, aktualizácie nájdete na:
http://samba.org/samba/patches/

Ďalšou možnosťou je pridať parameter:

nt pipe support = no

do sekcie [global] v smb.conf a reštartovať smbd. V tomto prípade ale berte na vedomie, že pridanie tohto parametra môže mať dopad na niektoré funkcie systémov Windows.

Ak používate RedHat, oprava zraniteľnosti bola uskutočnená v RHEL 7, RHEL 6, RHEL 5 ELS

Ak používate Debian, oprava zraniteľnosti bola uskutočnená v Debian 8 a Debian 7

Zdroje

http://blog.blackducksoftware.com/cve-2017-7494-dancing-samba-vulnerability
https://www.samba.org/samba/security/CVE-2017-7494.html
https://rhn.redhat.com/errata/RHSA-2017-1270.html
https://security-tracker.debian.org/tracker/CVE-2017-7494

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
Národná jednotka reakcie
na núdzové počítačové situácie

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-04V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Cisco Web Security Appliance Command Injection and Privilege Escalation Vulnerability

Popis

Ide o zraniteľnosť vo webovom rozhraní zariadenia Cisco Web Security Appliance (WSA), ktorá umožňuje autentifikovanému vzdialenému útočníkovi vykonať škodlivý kód a zvýšiť oprávnenia na root. Útočník sa musí overiť pomocou platných poverení administrátora.

Zraniteľnosť je dôsledkom nedostatočného overenia vstupov poskytnutých používateľmi na webovom rozhraní. Útočník by túto chybu zabezpečenia mohol zneužiť autentifikáciou na postihnuté zariadenie a vykonaním škodlivého kódu cez webové rozhranie. Exploit môže dovoliť útočníkovi, aby zvýšil privilégiá od administrátora po root.

CVE

CVE-2017-6746

CISCO Bug ID

CSCvd88862

Zasiahnuté systémy

Cisco AsyncOS Software 10.0 a novšie pre WSA na virtuálnych aj hardvérových zariadeniach

Následky

Neoprávnené spustenie škodlivého kódu, zvýšenie privilégií pre root

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu Cisco AsyncOS Software na najnovšiu verziu, nakoľko táto zraniteľnosť bola spoločnosťou Cisco opravená a neexistuje žiadne iné riešenie, ako zabrániť zneužitiu zraniteľnosti.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170719-wsa1

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
Národná jednotka reakcie
na núdzové počítačové situácie

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-05V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Vulnerabilities in Oracle Outside In Technology affect IBM WebSphere Portal

Popis

Ide o niekoľko zraniteľností v zabezpečení technológie Oracle Outside In Technology, ktoré majú vplyv na IBM WebSphere Portal. Je to súbor zraniteľností, ktoré boli opravené a tieto opravy sú obsiahnuté v aktualizáciách produktov.

CVE

CVE-2016-5558, CVE-2016-5574, CVE-2016-5577, CVE-2016-5578, CVE-2016-5579, CVE-2016-5588

Zasiahnuté systémy

WebSphere Portal 8.5
WebSphere Portal 8.0
WebSphere Portal 7
WebSphere Portal 6.1

Následky

Odporúčania

Odporúčame bez meškania vykonať aktualizáciu vyššie zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg21994838

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
Národná jednotka reakcie
na núdzové počítačové situácie

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 18. 07. 2017 – 25. 07. 2017

No: B20170725-06V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (W-~~G-A-R~~)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Oracle Critical Patch Update Advisory – Júl 2017

Popis

Critical Patch Update (CPU) je kolekcia aktualizácií pre viacero bezpečnostných zraniteľností. CPU pre júl 2017 obsahuje viacero významných aktualizácií zraniteľností, ktoré zasahujú viacero produktov.

Zasiahnuté systémy

Celý zoznam zasiahnutých systémov nájdete na:
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

Následky

Odporúčania

Odporúčame bez meškania skontrolovať, ktoré zo systémov uvedených v zozname používate a následne vykonať ich aktualizáciu.

Zdroje

http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.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
Národná jednotka reakcie
na núdzové počítačové situácie