Mesačný prehľad kritických zraniteľností
Marec 2017

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2017-0021 vo Windows Hyper-V je spôsobená chybami pri overovaní paketov vSMB. Umožňuje vzdialené spustenie škodlivého kódu. Útočník vo vnútri virtuálneho stroja spustením špeciálnej aplikácie dokáže spustiť ľubovoľný kód na Hyper-V hostiteľskom operačnom systéme.

Zraniteľnosti CVE-2017-0075 a CVE-2017-0109 vo Windows Hyper-V sú spôsobené chybami pri schvaľovaní vstupu overovaného používateľa. Umožňujú vzdialené spustenie škodlivého kódu. Útočník spustením špeciálnej aplikácie v hosťovanom operačnom systéme (guest) dokáže spustiť ľubovoľný kód na Hyper-V hostiteľskom operačnom systéme.

Zraniteľnosť CVE-2017-0023 v Microsoft Windows PDF library je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením.

Zraniteľnosti CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 a CVE-2017-0148 na Microsoft Server Message Block 1.0 (SMBv1) serveroch sú spôsobené chybami pri spracovaní určitých požiadaviek. Umožňujú spustenie ľubovoľného kódu na cieľovom serveri. Vo väčšine prípadov na exploitovanie zraniteľnosti stačí, keď vzdialený neautentifikovaný útočník pošle špeciálny paket cieľovému SMBv1 serveru.

Zraniteľnosti CVE-2017-0072, CVE-2017-0083, CVE-2017-0084, CVE-2017-0086, CVE-2017-0087, CVE-2017-0088, CVE-2017-0089 a CVE-2017-0090 vo Windows Uniscribe sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením.

Zraniteľnosť CVE-2017-0104 v iSNS Server je spôsobená chybami pri schvaľovaní vstupu od klienta. Umožňuje vzdialené spustenie škodlivého kódu na úrovni systémového používateľa.

Zraniteľnosti CVE-2017-0108 a CVE-2017-0014 vo Windows Graphics Component sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením. Zraniteľnosť CVE-2017-0014 bola publikovaná verejne.

Zraniteľnosť CVE-2017-0005 vo Windows Graphics Device Interface je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje zvýšenie privilégii. Útočník po prihlásení do systému dokáže spustením škodlivej aplikácie získať kontrolu nad systémom. Bolo zaznamenané zneužitie tejto zraniteľnosti.

Zraniteľnosť CVE-2017-0022 v Microsoft XML Core Services je spôsobená chybami pri práci s objektmi v pamäti. Umožňuje prezeranie súborov na disku po navštívení webstránky a bolo zaznamenané jej zneužitie.

Spoločnosť Microsoft taktiež zverejnila opravy kritických zraniteľností integrovaného prehrávača Adobe Flash Player.

Zraniteľné systémy:
Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit Systems
Windows 8.1 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1511 for x32-based Systems
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for x32-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 for Itanium-based Systems Service Pack 2
Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016 for x64-based Systems
Windows Server 2016 for x64-based Systems (Server Core installation)

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS17-008, MS17-009, MS17-010, MS17-011, MS17-012, MS17-013, MS17-022 a taktiež aj MS17-023, ktorá obsahuje novú verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko bol zaznamenaný výskyt exploitov na niektoré z uvedených zraniteľnosti.
Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-008.aspx
https://technet.microsoft.com/en-us/library/security/ms17-009.aspx
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://technet.microsoft.com/en-us/library/security/ms17-011.aspx
https://technet.microsoft.com/en-us/library/security/ms17-012.aspx
https://technet.microsoft.com/en-us/library/security/ms17-013.aspx
https://technet.microsoft.com/en-us/library/security/ms17-022.aspx
https://technet.microsoft.com/en-us/library/security/ms17-023.aspx

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2017-0108 a CVE-2017-0014 vo Windows Graphics Component sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu. Útočník môže zneužitím tejto zraniteľnosti prevziať kontrolu nad zariadením. Zraniteľnosť CVE-2017-0014 bola publikovaná verejne.

Zraniteľnosti CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE-2017-0030, CVE-2017-0031, CVE-2017-0052 a CVE-2017-0053 sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu.

Zraniteľnosť CVE-2017-0110 v Microsoft Exchange Outlook Web Access je spôsobená chybami pri práci s webovými požiadavkami. Umožňuje zvýšenie privilégií po kliknutí na škodlivý odkaz a útočník dokáže odhaliť citlivé informácie používateľa.

Zraniteľné systémy:
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2016 (32-bit editions)
Microsoft Office 2016 (64-bit editions)

Microsoft Office for Mac 2011
Microsoft Office 2016 for Mac
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Viewer

Microsoft SharePoint Server 2007 Service Pack 3 (32-bit edition)
Microsoft SharePoint Server 2007 Service Pack 3 (64-bit edition)
Microsoft SharePoint Server 2010 Service Pack 2
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft Office Web Apps 2010 Service Pack 2

Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Lync for Mac 2011

Microsoft Exchange Server 2013 Service Pack 1
Microsoft Exchange Server 2013 Cumulative Update 14
Microsoft Exchange Server 2016 Cumulative Update 3

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS17-013, MS17-014 a MS17-015. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-013.aspx
https://technet.microsoft.com/en-us/library/security/ms17-014.aspx
https://technet.microsoft.com/en-us/library/security/ms17-015.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 12 zraniteľností, z ktorých je 5 označených ako kritické, sú spôsobené chybami pri práci s objektmi v pamäti. Umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej webstránky.

Zraniteľné systémy:
Microsoft Internet Explorer 9
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS17-006. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-006.aspx

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 32 zraniteľností, z ktorých je 20 označených ako kritické, sú spôsobené chybami pri práci s objektami v pamäti. Umožňujú vzdialené spustenie školivého kódu po navštívení infikovanej webstránky.

Zraniteľné systémy:
Microsoft Edge

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS17-007. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si marcové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-007.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala dve aktualizácie prehliadača Firefox opravujúce 8 kritických zraniteľností umožňujúcich vzdialené spustenie škodlivého kódu, spôsobenie pádu aplikácie alebo obchádzanie bezpečnostných mechanizmov po navštívení infikovaných webstránok.

Zraniteľné systémy:
Mozilla Firefox 52 a predchádzajúce
Mozilla Firefox ESR 52

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 52.0.1 a Mozilla Firefox ESR 52.0.1)
Aktualizácia prehliadača by sa mala nainštalovať automaticky, pokiaľ sa tak nestalo, aktualizujte manuálne kliknutím na Firefox menu, ponuku Pomocníka a O prehliadači Firefox. Zobrazí sa okno s informáciou o používanej verzii prehliadača, súčasne sa skontrolujú a následne stiahnu aktualizácie.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/mfsa2017-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/

Google Chrome

Spoločnosť Google zverejnila tri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 41 bezpečnostných zraniteľností.
Najvážnejšie zraniteľnosti môžu spôsobiť pád aplikácie, únik citlivých informácií, alebo iný bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo otvorení infikovaného PDF súboru.

Zraniteľné systémy:
Google Chrome verzie 57.0.2987.133 a nižšej

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 58.0.3029.81. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop_29.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 8 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobné pretečením pamäte, použitím uvoľnenej pamäte, chybami pri práci s objektmi v pamäti a ďalšími chybami. Tieto zraniteľnosti umožňujú útočníkovi vzdialené spustenie škodlivého kódu či odhalenie potenciálne citlivých informácii. Útočník zneužitím týchto zraniteľností dokáže prevziať kontrolu nad systémom.

Zraniteľné systémy:
Adobe Flash Player verzie 24.0.0.221 a nižšej

Odporúčania:
Všetkým používateľom odporúčame aktualizovať Adobe Flash Player na verziu 25.0.0.127 čo najskôr.
Aktualizácie sú dostpuné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostrednictvom kontroly dostupných aktualizácií v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb17-07.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci marec nevydala opravy žiadnych zraniteľností platformy Microsoft .NET.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms17-mar.aspx

Oracle Java

Spoločnosť Oracle v mesiaci marec nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 18. apríl 2017.

Zdroje:
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

6. Iné závažné zraniteľnosti

VMware

Zraniteľnosti CVE-2017-4902 a CVE-2017-4903 umožňujú spustenie útočníkovho kódu na hostiteľovi v prípade kompromitácie virtualizovaného zariadenia. Zraniteľnosti zneužívajú pretečenie bufferu na halde a použitie neinicializovanej pamäte v komponente SVGA.

Zraniteľnosť CVE-2017-4904 umožňuje spustenie útočníkovho kódu na hostiteľovi v prípade kompromitácie virtualizovaného zariadenie. Zraniteľnosť zneužíva využívanie neinicializovanej pamäte v komponente XHCI Controller

Zraniteľné systémy:
ESXi 5.5,6.0 U1, 6.0 U2, 6.0 U3, 6.5
Vmware Workstation 12.x

Odporúčania:
Správcom systémov odporúčame nainštalovať záplaty na uvedené zraniteľnosti. Popis záplat pre jednotlivé verzie je uvedené na https://www.vmware.com/security/advisories/VMSA-2017-0006.html.

Zdroje:
https://www.vmware.com/security/advisories/VMSA-2017-0006.html

SAP

Zraniteľnosť CVE-2017-6950 umožňuje v dôsledku konfigurácie SAP GUI spúšťať program regsvr32.exe, ktorý môže následne načítať a spustiť škodlivé DLL knižnice zo zdieľaného úložiska.
Uvedená zraniteľnosť môže byť zneužitá na spustenie škodlivého kódu na koncových zariadeniach (klientoch využívajúcich SAP GUI) a na prístup k ľubovoľným súborom a adresárom a informáciám uložených v zraniteľnom SAP systéme.

Na zneužitie tejto zraniteľnosti musí útočník najprv kompromitovať SAP server. Môže ku tomu využiť viacero známych zraniteľností, z ktorých niektoré ešte nie sú opravené. Následne môže zneužiť uvedenú zreniteľnosť v SAP GUI a vytvoriť škodlivú transakciu, pomocou ktorej infikuje klientske zariadenia malvérom. Je pravdepodobné, že táto zraniteľnosť je, resp. bude zneužívaná na šírenie ransomvéru a iných druhov škodlivého kódu.

Odporúčania:
Správcom systémov odporúčame nainštalovať záplatu na uvedenú zraniteľnosť, ktorý vyšla v mesiaci marec pod označením 2407616 (SAP Security Note). Zároveň odporúčame zabezpečiť klientske zariadenia antimalvér riešením a zablokovať akýkoľvek prístup na SAP server z prostredia Internetu, resp. z externých sietí.
Návod na aktualizáciu SAP GUI je dostupný na stránke https://erpscan.com/press-center/blog/sap-security-notes-march-2017/

Zdroje:
https://erpscan.com/sap-ransomware/
https://erpscan.com/advisories/erpscan-17-011-sap-gui-versions-remote-code-execution-bypass-security-policy/

Vault 7

Na server WikiLeaks bola zverejnená časť materiálov, ktorá údajne unikla americkej službe CIA. Dokumenty sú publikované pod názvom Vault 7 a obsahujú viaceré informácie v oblasti vývoja kybernetických útočných nástrojov. Jedná sa prevažne o rôzne druhy škodlivého kódu, napr. trójske kone, nástroje na vzdialenú kontrolu systémov a 0-day exploity používané na prienik do zariadení, ich infikovanie (implantáciu), získanie kontroly nad nimi a krádež informácií. 0-day exploity sú zamerané na produkty amerických a európskych firiem, vrátane Apple iPhone, Google Android, Microsoft Windows a smart TV od Samsungu. V súčasnosti *WikiLeaks* zverejnili prvú časť materiálov *Vault 7*, nazvanú **Year Zero**, ktorá údajne pokrýva aktivity CIA v roku 2016.

Na základe vyjadrení Microsoftu však väčšina exploitov nefunguje na aktuálnych systémoch. Taktiež viaceré antivírové spoločnosti už sú schopné detekovať uvedený škodlivý kód.
Nie je však vylúčené, že mnohé mobilné zariadenia a televízory sú stále zraniteľné z dôvodu nedostatočného aktualizačného procesu.

Odporúčania:
Administrátorom systémov odporúčame pravidelne aktualizovať všetok používaný softvér na zariadeniach pod ich správou. Nepoužívaný softvér odporúčame odinštalovať.
Používateľom odporúčame navštevovať iba dôveryhodné stránky a neklikať na odkazy v e-mailoch pochádzajúcich z nedôveryhodných zdrojov.