Mesačný prehľad kritických zraniteľností
Február 2016

1. Operačné systémy Microsoft Windows

Zraniteľnosť CVE-2016-0046 vo Windows Reader umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru.

Zraniteľnosť CVE-2016-0058 vo Windows PDF knižnici je spôsobená nesprávnym spracovaním API volaní a umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného PDF súboru.

Zraniteľnosť CVE-2016-0038 aplikácie Windows Denník (Journal) je spôsobená chybou pri spracovaní súborov Windows Denník (.jnt) a umožňuje vzdialené spustenie škodlivého kódu po otvorení infikovaného súboru Windows Denník.

Zraniteľnosti CVE-2016-0041 a CVE-2016-0042 sú spôsobené chybami pri načítavaní dynamicky linkovaných knižníc a umožňujú útočníkovi s platnými prihlasovacími údajmi zvýšenie oprávnení a prevzatie kontroly nad systémom po spustení infikovanej aplikácie.

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 32-bit Systems
Windows 10 Version 1511 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 for Itanium-based Systems Service Pack 2
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 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)

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS16-012, MS-013 a MS16-014. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko niektoré zraniteľnosti boli publikované verejne a použitie exploitov na uvedené zraniteľnosti je pravdepodobné.
Správcom systémov odporúčame prezrieť si februárové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Upozornenie:
Pokiaľ používate operačný systém Microsoft Windows 8, odporúčame prejsť na novšiu verziu (napr. Windows 8.1), prípadne downgradovať na Windows 7 SP1, pretože pre systémy Windows 8 už nebudú vychádzať aktualizácie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-012.aspx
https://technet.microsoft.com/en-us/library/security/ms16-013.aspx
https://technet.microsoft.com/en-us/library/security/ms16-014.aspx
https://support.microsoft.com/en-gb/lifecycle?C2=16796

2. Kancelárske balíky Microsoft Office a Office Web Apps

Zraniteľnosti CVE-2016-0022, CVE-2016-0052, CVE-2016-0053, CVE-2016-0054, CVE-2016-0055 a CVE-2016-0056 spôsobené chybami pri práci s objektmi v pamäti počas spracovania dokumentov Office umožňujú útočníkovi vzdialené spustenie škodlivého kódu s oprávneniami užívateľa po otvorení infikovaného súboru.

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

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

Microsoft SharePoint Server 2007 Service Pack 3
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

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-015. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je pravdepodobný.
Správcom systémov odporúčame prezrieť si februárové Microsoft Security Bulletin dostupné na odkazoch nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-015.aspx

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft vydala sadu záplat na 13 zraniteľností, z ktorých 7 je označených ako kritických, sú spôsobené chybami pri práci s pamäťou a pri načítavaní dynamických knižníc a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Internet Explorer 9-11

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-009. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-009.aspx

Microsoft Edge

Spoločnosť Microsoft vydala jednu sadu záplat na 6 zraniteľnosti, z ktorých sú 4 označené ako kritické, sú spôsobené chybami pri práci s pamäťou a umožňujú vzdialené spustenie škodlivého kódu po navštívení infikovanej stránky.

Zraniteľné systémy:
Microsoft Edge

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-011. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom

systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupné na odkaze nižšie.

Zdroj:
https://technet.microsoft.com/en-us/library/security/ms16-011.aspx

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúce 2 kritické zraniteľnosti.

Zraniteľnosť CVE-2016-1523 v knižnici Graphite 2 je spôsobená nesprávnou kontrolou interných parametrov, čo môže byť zneužité na vzdialené spustenie škodlivého kódu prostredníctvom infikovaného fontu.

Zraniteľnosť CVE-2016-1949 je spôsobená nesprávnym obmedzovaním komunikácie medzi rozšíreniami a Service Workers a môže byť zneužitá na obídenie ochrany Same Origin Policy pomocou infikovanej stránky využívajúcej NPAPI.

Zraniteľné systémy:
Mozilla Firefox 44.0.1 a predchádzajúce
Mozilla Firefox ESR 38.6 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 44.0.2 a Mozilla Firefox ESR 38.6.1)
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/sk/security/advisories/

Google Chrome

Spoločnosť Google zverejnila tri aktualizácie prehliadača Chrome, ktoré obsahujú opravy 7 bezpečnostných zraniteľností.

Kritická zraniteľnosť CVE-2016-1629 umožňuje obísť ochranu Same Origin a uniknúť zo sandboxu prehliadača.

Ostatné vážne zraniteľnosti umožňujú spôsobiť pád aplikácie alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných webstránok alebo PDF súborov.

Zraniteľné systémy
Google Chrome do verzie 48.0.2564.109 a predchádzajúce

Odporúčania:
Odporúčame aktualizovať prehliadač na verziu 48.0.2564.116. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:
http://googlechromereleases.blogspot.in/2016/02/stable-channel-update.html
http://googlechromereleases.blogspot.in/2016/02/stable-channel-update_9.html
http://googlechromereleases.blogspot.in/2016/02/stable-channel-update_18.html

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 22 zraniteľnosti, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené opätovným použitím uvoľnenej pamäte, použitím nesprávnych typov premenných, pretečením pamäte, pretečením pamäte a ďalšími chybami pri práci s pamäťou. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód pomocou infikovaného Flash obsahu.

Zraniteľné systémy:
Adobe Flash Player verzie 20.0.0.286 a nižšej
Adobe Flash Player verzie 18.0.0.326 a nižšej
Adobe Flash Player verzie 11.2.202.559 a nižšej

Odporúčania:
Používateľom Windows odporúčame aktualizovať Adobe Flash Player na verziu 20.0.0.306, používateľom Adobe Plash Player s predĺženou podporou odporúčame aktualizovať na verziu 18.0.0.329. Používateľom Linux odporúčame aktualizovať na verziu 11.2.202.569.
Aktualizáciu odporúčame vykonať čo najskôr.
Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácii v produkte Adobe Flash Player.

Zdroje:
https://helpx.adobe.com/security/products/flash-player/apsb16-04.html

5. Frameworky

Microsoft .NET Framework

Spoločnosť Microsoft v mesiaci nevydala opravy žiadnych kritických zraniteľností platformy .NET. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosti umožňujúce spôsobiť pád systému alebo únik informácií.

Zraniteľné systémy:
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5/3.5.1

Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6/4.6.1

Odporúčania:
Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS16-019. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér. Správcom systémov odporúčame prezrieť si februárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:
https://technet.microsoft.com/en-us/library/security/ms16-019.aspx

Oracle Java

Spoločnosť Oracle v mesiaci február nevydala žiadne aktualizácie platformy Java. Najbližšia veľká sada aktualizácií je naplánovaná na 19. apríl 2016.

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

6. Iné závažné zraniteľnosti

Zraniteľnosti v knižnici GNU C Library

V knižnici GNU C Library bolo objavených viacero zraniteľností pretečenia zásobníka, ktoré umožňujú útočníkovi spôsobiť pád aplikácie alebo vzdialené spustenie kódu pomocou zaslania špeciálne upravenej DNS odpovede.

Zraniteľné systémy:
libc / libc6 pred 2.23

Odporúčania:
Záplata na uvedenú zraniteľnosť bola zverejnená v bezpečnostných aktualizáciách jednotlivých linuxových distribúcií. Odporúčame preto skontrolovať dostupnosť aktualizácií balíka glibc (prípadne libc6) a ich nainštalovanie.

Zdroje:
http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=145

DROWN útok

DROWN útok umožňuje útočníkovi dešifrovať zachytenú komunikáciu zabezpečenú pomocou SSL/TLS protokolu.

Útok umožňuje dešifrovať zachytenú komunikáciu zabezpečenú pomocou SSL/TLS protokolu. Útočník môže následne odpočúvať komunikáciu medzi klientom a serverom a môže tak

získať prístup k prenášaným údajom, napr. sa môže jednať o používateľské mená a heslá, obsah emailov, osobné a finančné údaje.

Zraniteľné systémy:

- služby so zapnutou podporou protokolu SSLv2
- služby, ktoré používajú rovnaký privátny kľúč ako iné služby so zapnutou podporou protokolu SSLv2

Odporúčania:

- Zakázať podporu SSLv2 (odporúčame nechať zapnutú podporu iba pre TLSv1.1 a TLSv1.2).
- Návody pre bežné produkty je možné nájsť na https://drownattack.com/#mitigation
- Nepoužívať rovnaký privátny kľúč/certifikát pre viaceré služby/servery (web, SMTP, IMAP, POP,...).
- Otestovať všetky služby (verejné aj interné) využívajúce SSL/TLS na prítomnosť tejto zraniteľnosti.

Zdroje:

http://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=146
https://drownattack.com/