

Mesačný prehľad kritických zraniteľností

Január 2017

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft v mesiaci január nevydala opravy žiadnych kritických zraniteľností OS Windows.. Boli však zverejnené opravy kritických zraniteľností integrovaného prehrávača Adobe Flash Player a dôležité aktualizácie opravujúce zraniteľnosť CVE-2017-0004.

Zraniteľnosť CVE-2017-0004 v subsysteme LSASS je spôsobená chybami pri spracovaní autentifikačných žiadostí. Umožňuje spôsobiť pád systému a vynútiť reštart odoslaním infikovanej autentifikačnej žiadosti. Zraniteľnosť bola publikovaná verejne.

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 10 Version 1607 for 32-bit 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 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 R2
- Windows Server 2016 for 64-bit Systems

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označeniami MS17-004, a taktiež aj MS17-003, ktorá obsahuje novú verziu Adobe Flash Player. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľností je pravdepodobný. Správcov systémov odporúčame prezrieť si januárové Microsoft Security Bulletin dostupné na odkazoch nižšie.

V januári taktiež skončila podpora pre Microsoft SQL Server 2012 Service Pack 2. Správcom odporúčame prejsť na novšiu verziu Service Packu alebo novšiu verziu samotného SQL Servera.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms17-004.aspx>

<https://technet.microsoft.com/en-us/library/security/ms17-003.aspx>

<https://support.microsoft.com/en-us/help/4001737/products-reaching-end-of-support-for-2017>

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft v mesiaci január nevydala opravy žiadnych kritických zraniteľností Microsoft Office. Boli však zverejnené dôležité aktualizácie opravujúce zraniteľnosť CVE-2017-0003.

Zraniteľnosť CVE-2017-0003 je spôsobená chybami pri práci s objektmi v pamäti umožňuje vzdialené spustenie škodlivého kódu po navštívení webstránky alebo otvorení infikovaného dokumentu.

Zraniteľné systémy:

Microsoft Office 2016 (32-bit edition)

Microsoft Office 2016 (64-bit edition)

Microsoft SharePoint Enterprise Server 2016

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS17-002. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na niektoré z uvedených zraniteľností je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si januárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms17-002.aspx>

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft v mesiaci január nevydala opravy žiadnych zraniteľností prehliadača Microsoft Internet Explorer.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms17-jan.aspx>

Mesačný prehľad kritických zraniteľností

Microsoft Edge

Spoločnosť Microsoft vydala sadu záplat na 1 zraniteľnosť, z ktorých žiadna nie je označená ako kritická. Opravená zraniteľnosť CVE-2017-0002 umožňovala obídenie cross-domain obmedzení a vloženie škodlivého obsahu z webstránok jednej domény do druhej a bola publikovaná verejne.

Zraniteľné systémy:

Microsoft Edge

Odporúčania:

Spoločnosť Microsoft zverejnila pravidelnú mesačnú aktualizáciu prostredníctvom bežného kanála Windows Update. Záplaty na uvedené zraniteľnosti sú distribuované pod označením MS17-001. Odporúčame všetkým používateľom čo najskôr aktualizovať zraniteľný softvér, nakoľko výskyt exploitov na uvedené zraniteľnosti je vysoko pravdepodobný. Správcom systémov odporúčame prezrieť si januárový Microsoft Security Bulletin dostupný na odkaze nižšie.

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms17-001.aspx>

Mozilla Firefox

Spoločnosť Mozilla vydala jednu aktualizáciu prehliadača Firefox opravujúcu 3 kritické zraniteľnosti umožňujúce vzdialené spustenie škodlivého kódu, spôsobiť pád aplikácie, obídenie bezpečnostných mechanizmov alebo ďalšie bližšie nešpecifikované dopady po navštívení infikovaných webstránok.

Zraniteľné systémy:

Mozilla Firefox 51.1 a predchádzajúce
Mozilla Firefox ESR 45.6

Odporúčania:

Odporúčame aktualizovať jednotlivé programy na najnovšie verzie (Mozilla Firefox 51.0.1, resp. Mozilla Firefox ESR 45.7).

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/mfsa2017-01/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/>

Google Chrome

Spoločnosť Google zverejnila dve aktualizácie prehliadača Chrome, ktoré obsahujú opravy 51 bezpečnostných zraniteľností.

Mesačný prehľad kritických zraniteľností

Najväčšie zraniteľnosti umožňujú spôsobiť pád aplikácie, XSS, únik citlivých informácií alebo iný, bližšie nešpecifikovaný dopad po načítaní infikovaných.

Zraniteľné systémy

Google Chrome verzie 55.0.2883.87 a nižšej

Odporúčania:

Odporúčame aktualizovať prehliadač na verziu 56.0.2924.76, prípadne 56.0.2924.87. Aktualizácie sú dostupné prostredníctvom štandardných kanálov.

Zdroje:

<https://googlechromereleases.blogspot.sk/2017/01/stable-channel-update-for-desktop.html>

4. Adobe Flash Player

Spoločnosť Adobe zverejnila jednu aktualizáciu opravujúcu 13 zraniteľností, všetky sú označené ako kritické.

Zraniteľnosti sú spôsobené použitím opätovným použitím uvoľnenej pamäte, pretečením pamäte, chybami pri práci s objektami v pamäti a ďalšími chybami. Tieto zraniteľnosti umožňujú vzdialenému útočníkovi spustiť škodlivý kód alebo obchádzať bezpečnostné mechanizmy pomocou infikovaného Flash obsahu. Exploity na zraniteľnosť CVE-2017-2930 sú verejne dostupné.

Zraniteľné systémy:

Adobe Flash Player verzie 24.0.0.186 a nižšej

Odporúčania:

Všetkým používateľom odporúčame aktualizovať Adobe Flash Player na verziu 24.0.0.194. Aktualizáciu odporúčame vykonať čo najskôr, nakoľko boli exploity na niektoré uvedené zraniteľnosti publikované verejne.

Aktualizácie sú dostupné prostredníctvom stránky Adobe Flash Player Download Center, prípadne prostredníctvom kontroly dostupných aktualizácií v produkte Adobe Flash Player.

Zdroje:

<https://helpx.adobe.com/security/products/flash-player/apsb17-02.html>

5. Frameworky

Microsoft .NET Framework

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

Zdroje:

<https://technet.microsoft.com/en-us/library/security/ms17-jan.aspx>

Oracle Java

Spoločnosť Oracle v mesiaci január vydala bezpečnostnú aktualizáciu platformy Java opravujúcu 17 zraniteľností, z ktorých sú 3 kritické.

Zraniteľnosti CVE-2017-3289, CVE-2017-3272 a CVE-2017-3241 umožňujú vzdialenému útočníkovi bez autentifikácie spustiť škodlivý kód, kompromitáciu zariadenia, alebo iné bližšie neurčené dopady.

Zraniteľné systémy:

Java SE 6u131

Java SE 7u121

Java SE 8u111

Odporúčania:

Spoločnosť Oracle zverejnila aktualizáciu prostredníctvom bežného kanála Java Auto Update. Aktualizácie sú dostupné aj na stránke java.com. Používateľom odporúčame nainštalovať najnovšiu verziu Java SE 8 Update 121.

Zdroje:

<http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html>