Mesačný prehľad kritických zraniteľností
Júl 2019

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 2 kritické zraniteľnosti.

Opravená bola zraniteľnosť CVE-2019-1102 v komponente Graphics Device Interface(GDI+). Táto zraniteľnosť vzniká pri pristupovaní komponentu ku objektom v pamäti a umožňuje vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať kontrolu nad zraniteľným systémom. Na napadnutie systému cez internet je potrebné, aby útočník hostil webovú stránku, ktorá je upravená na zneužitie tejto zraniteľnosti a aby presvedčil používateľa navštíviť ju (napríklad kliknutím na odkaz, ktorý na ňu smeruje). Napadnúť systém je možné aj cez zdieľanie dokumentu, ktorý je tiež upravený na zneužitie zraniteľnosti. Potom už len útočníkovi stačí presvedčiť používateľa, aby ho otvoril.

Ďalšia kritická zraniteľnosť CVE-2019-0785 sa týka DHCP servera. Útočník môže poškodiť pamäť, ak pošle špeciálne upravené DHCP pakety na DHCP server, ktorý je v móde „failover“. Po zneužití dokáže útočník vykonávať škodlivý kód na danom DHCP serveri alebo spôsobiť, aby DHCP služby neodpovedali.

Zraniteľné systémy:

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for 64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1903 for x64-based Systems
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 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 Itanium-Based Systems Service Pack 2
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 Itanium-Based Systems Service Pack 1
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 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1803 (Server Core Installation)

Odporúčania:
Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1102
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0785

2. Kancelárske balíky Microsoft Office a Office Web Apps

Tento mesiac nebola vydaná oprava na kritické zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps. Bolo opravených 7 závažných zraniteľností umožňujúcich vzdialené vykonávanie kódu, falšovanie identity a únik informácií.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila v mesiaci júl 6 kritických zraniteľností.

Zraniteľnosť CVE-2019-1001, CVE-2019-1056, CVE-2019-1059, CVE-2019-1004, CVE-2019-1063 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj nevhodne pristupuje ku objektom v pamäti. Útočník po zneužití zraniteľnosti získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti. Potom musí presvedčiť používateľa, aby navštívil danú stránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na vloženie infikovaného obsahu. Naviac, môže útočník vložiť ovládací prvok ActiveX označený ako „bezpečný pre inicializáciu“ do aplikácie alebo dokumentu Microsoft Office.

Zraniteľnosť CVE-2019-1104 vzniká pri pristupovaní prehliadačov ku objektom v pamäti. Na zneužitie zraniteľnosti útočník môže hostiť webstránku, ktorej obsah je prispôsobený na využitie tejto zraniteľnosti cez Interner Explorer. Potom sa mu musí podariť presvedčiť používateľa, aby otvoril škodlivú webstránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom na pridanie infikovaného súboru. Niekedy sa od používateľa očakáva aktívny prístup (kliknutie na odkaz,..). Zneužitie tejto zraniteľnosti umožňuje vzdialené vykonávanie kódu. Útočník získava rovnaké práva ako prihlásený používateľ. Ak je prihlásený administrátor, útočník získa práva administrátora a získa kontrolu nad celým systémom.

Zraniteľné systémy:

Microsoft Internet Explorer verzie 10

Microsoft Internet Explorer verzie 11

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1001
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1004
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1056
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1059
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1063

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1104

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac 5 kritických zraniteľností.

Zraniteľnosť CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107 umožňuje vzdialené vykonávanie kódu, ak skriptovací nástroj Chakra nevhodne pristupuje ku objektom v pamäti. Na zneužitie tejto zraniteľnosti je potrebné hostiť webstránku, ktorej obsah je prispôsobený na využitie danej zraniteľnosti. Potom musí presvedčiť používateľa, aby navštívil danú stránku. Útočník môže takisto využiť kompromitované webové stránky alebo webové stránky, ktoré prijímajú alebo hostia obsah alebo reklamy poskytované používateľom. Útočník tak získava rovnaké práva ako momentálne prihlásený používateľ. Ak je teda prihlásený administrátor, útočník môže získať kontrolu nad celým systémom.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzie 1809 v 32-bitových, 64-bitových verziách aj ARM64 verzii
Microsoft Edge v systémoch Windows Server 2019
ChakraCore
Windows 10 Version 1709 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems, x64-based Systems, ARM64-based Systems
Windows 10 Version 1903 for 32-bit Systems, x64-based Systems, for ARM64-based Systems
Windows 10 for 32-bit Systems, x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Microsoft Edge v systémoch Windows Server 2016
Windows 10 Version 1703 for 32-bit Systems, x64-based Systems

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:

https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1062
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1092
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1103
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1106
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1107

Mozilla Firefox

V mesiaci júl boli opravené 2 kritické zraniteľnosti a 4 závažné.

Kritické zraniteľnosti CVE-2019-11709 a CVE-2019-11710 spôsobujú poškodenie pamäti a ich zneužitie môže viesť ku vykonávaniu ľubovoľného kódu.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 68 / ESR 60.8

Odporúčania:

Odporúčame aktualizáciu na verziu 68 / ESR 60.8

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/

Google Chrome

V mesiaci júl bola vydaná oprava na 2 zraniteľnosti.

Závažná zraniteľnosť CVE-2019-5847 vzniká vo V8 a spôsobuje pád systému. Po zneužití strednej zraniteľnosti CVE-2019-5848 môže dôjsť ku prezradeniu dôverných informácií.

Zraniteľné systémy:

Google Chrome verzie staršie ako 75.0.3770.142

Odporúčania:

Odporúčame aktualizáciu na verziu 75.0.3770.142

Zdroje:

https://chromereleases.googleblog.com/2019
https://chromereleases.googleblog.com/2019/07/stable-channel-update-for-desktop.html

4. Adobe Flash Player, Acrobat a Reader

V júli nevydala spoločnosť Adobe opravu na žiadne zraniteľnosti v Adobe Flash Player ani v Adobe Acrobat a Reader.

Zdroje:
https://helpx.adobe.com/security.html

5. Frameworky

Microsoft .NET Framework

V mesiaci júl bola opravená 1 kritická zraniteľnosť.

Zraniteľnosť s číslom CVE-2019-1113 vzniká, keď softvér .NET neskontroluje zdrojové označenie súboru. Ak útočník zneužije túto zraniteľnosť, získava rovnaké práva ako momentálne prihlásený používateľ a dokáže s danými právami vykonávať ľubovoľný kód. Ak je prihlásený používateľ s administrátorskými právami, útočník získava kontrolu nad celým systémom. Zneužitie danej zraniteľnosti vyžaduje, aby používateľ otvoril špeciálne upravený škodlivý súbor na zariadení so zraniteľnou verziou softvéru. V prípade emailového napadnutia, môže útočník škodlivý súbor odoslať používateľovi a presvedčiť ho, aby súbor otvoril.

Zraniteľné systémy:

Microsoft .NET Framework 2.0
Microsoft .NET Framework 3.0
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.7
Microsoft .NET Framework 4.7.1
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8

Odporúčania:

Odporúčame aplikovať aktualizácie publikované prostredníctvom služby Windows Update. Číslo aktualizácie pre konkrétny systém možno vyhľadať na prvom z nižšie uvedených odkazov vložením identifikátora zraniteľnosti do vyhľadávania.

Zdroje:
https://portal.msrc.microsoft.com/en-us/security-guidance
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1113

Oracle Java

Spoločnosť Oracle vydala v mesiaci júl plánovanú štvrťročnú veľkú sadu aktualizácií. V produkte Java SE a Java SE Embedded bola opravená 1 závažná zraniteľnosť CVE-2019-7317.

Zraniteľné systémy:

Java SE 7u211, 8u212, 11.0.3, 12.0.1
Java SE Embedded 8u211

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:

https://www.oracle.com/technetwork/topics/security/alerts-086861.html
https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html#AppendixJAVA

6. Iné závažné zraniteľnosti

Zraniteľnosť SACK Panic spôsobuje zrútenie linuxového systému

Spoločnosť Netflix zverejnila informácie o štyroch zraniteľnostiach v jadre operačného systému Linux, ktoré označila ako kritické. Zraniteľnosti súvisia s funkcionalitou TCP protokolu a nachádzajú sa v mechanizme SACK a parametri MSS. Útočník môže spôsobiť neúmerné vyťaženie systémových prostriedkov a nedostupnosť systému. Viac informácií na stránke.

Kritická zraniteľnosť Drupal 8.7.4 umožňuje prevziať kontrolu nad webstránkou

Kritická zraniteľnosť v manažéri obsahu webstránok Drupal umožňuje útočníkom pri návšteve stránky obísť autentifikáciu a získať nad ňou plnú kontrolu. Je spojená s modulom Workspaces. Zraniteľná je verzia Drupal 8.7.4.

Palo Alto - kritická zraniteľnosť umožňuje vzdialene vykonávať kód

V produktoch Palo Alto Networks GlobalProtect a GlobalProtect Gateway bola objavené kritická zraniteľnosť umožňujúca útočníkom vzdialene vykonávať kód. K tomu stačí poslať zraniteľnému zariadeniu špeciálne upravenú požiadavku, nakoľko používateľský vstup nie je vhodne ošetrený. Útočník nepotrebuje autentifikáciu.

Kritická zraniteľnosť Androidov umožňuje prevzatie kontroly nad zariadením

Systémy Android vo verziách 7 až 9 obsahujú kritickú zraniteľnosť, ktorú môže útočník zneužiť na vzdialené vykonávanie kódu privilegovaného procesu a prevzatie kontroly nad zariadením. Chyba umožňujúca zápis mimo povolenú hodnotu sa konkrétne nachádza v prehrávači Android Player a zneužiteľná je po spustení škodlivého video súboru.