Mesačný prehľad kritických zraniteľností
máj 2021

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci máj 3 kritické a 22 závažných zraniteľností.

Kritická zraniteľnosť CVE-2021-28476 sa vyskytuje vo virtualizačnom nástroji Hyper-V. Neautentifikovaný útočník je schopný vzdialene vykonávať ľubovoľný kód. Úspešným zneužitím zraniteľnosti by mohol útočník kompromitovať hostiteľské zariadenie alebo spôsobiť nedostupnosť služby.

Zraniteľnosť CVE-2021-31166 sa nachádza v zásobníku protokolu HTTP. Umožňuje vzdialenému útočníkovi vykonávať ľubovoľný kód na serveri s oprávneniami jadra. Neautentifikovaný útočník môže chybu zneužiť zaslaním špeciálne vytvoreného http paketu zraniteľnej službe.

Posledná kritická zraniteľnosť je CVE-2021-31194. Nachádza sa v medziprocesovom komunikačnom mechanizme Windows OLE Automation. Zneužitím môže dôjsť k vzdialenému vykonaniu kódu.

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 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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
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 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)
Windows Server, version 20H2 (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-2021-28476
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-31166
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2021-31194

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft opravila v mesiaci máj 15 závažných zraniteľností a žiadnu kritickú zraniteľnosť. Osem zo závažných zraniteľností (CVE-2021-28455, CVE-2021-28474, CVE-2021-31175, CVE-2021-31176, CVE-2021-31177, CVE-2021-31179, CVE-2021-31180 a CVE-2021-31181) umožňuje útočníkom vzdialené vykonávanie kódu. Zneužitím zraniteľností CVE-2021-26418, CVE-2021-28478 a CVE-2021-31172 v produktoch SharePoint môže dôjsť k umožneniu predstierania identity. Zraniteľnosti CVE-2021-31171, CVE-2021-31173, CVE-2021-31174 a CVE-2021-31178 môžu viesť k úniku informácií.

Zraniteľné systémy:

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2013 RT Service Pack 1

Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)

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

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft opravila tento mesiac v prehliadači Internet Explorer 1 kritickú zraniteľnosť. Nachádza sa v skriptovacom nástroji. Zneužitím môže dôjsť k poškodeniu pamäte a tiež vzdialenému vykonaniu kódu. Útočník ju môže zneužiť vytvorením škodlivej webovej stránky a presvedčením obete, aby podvrhnutú stránku navštívila.

Zraniteľné systémy:
Internet Explorer 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-2021-26419

Microsoft Edge

Spoločnosť Microsoft opravila tento mesiac v prehliadači Microsoft Edge 2 závažné zraniteľnosti. Zneužitím zraniteľnosti CVE-2021-31982 môže dôjsť k obídeniu bezpečnostných prvkov. Útočník môže zraniteľnosť CVE-2021-31937 zneužiť na eskaláciu privilégií.

Zraniteľné systémy:
Microsoft Edge (Chromium-based)

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

Mozilla Firefox

V mesiaci máj bola v prehliadači Firefox opravená 1 závažná zraniteľnosť.
V prehliadači Firefox ESR nebola opravená žiadna kritická ani závažná zraniteľnosť.

Závažná zraniteľnosť CVE-2021-29952 sa vyskytuje v komponentoch Web Render. Keď sú komponenty zničené, súbeh môže spôsobiť nedefinované správanie. Pri vynaložení dostatočného úsilia môže útočník vzdialene vykonávať kód.

Zraniteľné systémy:
Mozilla Firefox verzie staršej ako 88.0.1

Odporúčania:
Odporúčame aktualizáciu Firefox na verziu 88.0.1.

Zdroje:
https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-20/

Google Chrome

V mesiaci máj vydala spoločnosť Google opravu pre 21 závažných zraniteľností a žiadnu kritickú. Závažné zraniteľnosti sa väčšinou týkajú použitia odalokovaného miesta v pamäti, pretečenia medzipamäte haldy alebo prístupu k pamäti mimo povolených hodnôt. Zraniteľnosti sa nachádzajú v komponentoch WebAudio, WebRTC, TabStrip, WebUI, V8 a podobne.

Zraniteľné systémy:
Google Chrome verzie staršej ako 91.0.4472.77 pre Windows, Mac a Linux

Odporúčania:
Odporúčame aktualizáciu na verziu 91.0.4472.77 pre Windows, Mac a Linux.

Zdroje:
https://chromereleases.googleblog.com/2021
https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html

4. Adobe Flash Player, Acrobat a Reader

V produkte Adobe Acrobat a Reader bolo v máji opravených 10 kritických a 4 závažné zraniteľnosti.

Kritické zraniteľnosti CVE-2021-28557 a CVE-2021-28565 súvisia s čítaním mimo povolených hodnôt. Zraniteľnosti CVE-2021-28564, CVE-2021-21044, CVE-2021-21038 a CVE-2021-21086 sa týkajú zápisu mimo povolených hodnôt a môžu viesť k vykonaniu ľubovoľného kódu.

CVE-2021-28562, CVE-2021-28550 a CVE-2021-28553 súvisia s použitím odalokovaného miesta v pamäti. Zneužitím sú útočníci schopní vzdialene vykonávať ľubovoľný kód. Zraniteľnosť CVE-2021-28560 sa týka pretečenia medzipamäte haldy, a tiež môže viesť ku vykonaniu ľubovoľného kódu.

Adobe prestala vydávať záplaty pre Flash Player 31. decembra 2020, teda nie je bezpečné ho používať.

Zraniteľné systémy:
Acrobat DC
Acrobat Reader DC
Acrobat 2020
Acrobat Reader 2020
Acrobat 2017
Acrobat Reader 2017

Odporúčania:
Odporúčame aktualizáciu:
Acrobat DC na verziu 2021.001.20155
Acrobat Reader DC na verziu 2021.001.20155
Acrobat 2020 na verziu 2020.001.30025
Acrobat Reader 2020 na verziu 2020.001.30025
Acrobat 2017 na verziu 2017.011.30196
Acrobat Reader 2017 na verziu 2017.011.30196

Zdroje:
https://helpx.adobe.com/security.html
https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

5. Frameworky

Microsoft .NET Framework

V mesiaci máj spoločnosť Microsoft opravila 1 závažnú a žiadnu kritickú zraniteľnosť vo frameworku .NET. Zneužitím CVE-2021-31204 môže dôjsť k eskalácii privilégií.

Zraniteľné systémy:
.NET 5.0
.NET Core 3.1

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

Oracle Java

Veľká sada opráv je plánovaná na 20. júl 2021.

Zdroje:
https://www.oracle.com/security-alerts/

6. Iné závažné zraniteľnosti

QNAP NAS – celosvetovo zneužívané zraniteľnosti sieťových úložísk

CSIRT.SK prináša súhrn zraniteľností a informácie o aktuálnych a minulých ransomvérových kampaniach, ktoré cielia na zariadenia QNAP NAS. Zariadenia, ktoré poskytujú sieťové úložisko s prístupom z internetu sú veľkým lákadlom pre útočníkov. Závažné bezpečnostné zraniteľnosti môžu umožniť potencionálnym útočníkom prevziať kontrolu nad zraniteľným NAS zariadením, odcudziť dáta, zneužiť zariadenie na šírenie rôzneho malvéru, a tak kompromitovať rozsiahlejšiu časť infraštruktúry organizácie. Viac informácií na stránke.

V softvéri Cisco SD-WAN vManage bolo opravených 5 zraniteľností

Spoločnosť Cisco vydala opravné aktualizácie pre 5 zraniteľností v softvéri Cisco SD-WAN vManage, pričom 2 z nich sú kritické. Vo všeobecnosti tieto zraniteľnosti môžu neautentifikovanému útočníkovi umožniť vzdialené vykonanie kódu alebo získať prístup k citlivým informáciám. Autentifikovanému lokálnemu útočníkovi umožňujú eskalovať privilégiá alebo získať neautorizovaný prístup k aplikáciám. Viac informácií na stránke.

Spoločnosť Cisco opravila 2 zraniteľnosti v softvéri HyperFlex HX

V softvéri Cisco HyperFlex HX boli nájdené a opravené 2 zraniteľnosti. Vo všeobecnosti tieto chyby môžu útočníkovi umožniť vzdialene vykonať ľubovoľný kód ako administrátor alebo používateľ tomcat8. Zraniteľné sú zariadenia Cisco so softvérom HyperFlex HX verzie 4.0, 4.5 a nižšej ako 4.0. Viac informácií na stránke.

F5 Networks – zariadenia BIG-IP obsahujú závažnú bezpečnostnú zraniteľnosť

Výskumníci spoločnosti Silverfort objavili závažnú bezpečnostnú zraniteľnosť v produkte BIG-IP spoločnosti F5 Networks. Zraniteľnosť existuje z dôvodu nedostatočnej implementácie protokolu Kerberos v manažmente prístupu APM produktov BIG-IP. Úspešné zneužitie zraniteľnosti by mohlo útočníkovi umožniť obísť proces autentifikácie, neoprávnene sa prihlásiť k rôznym službám, či

administrátorskej konzole zariadenia, a tak kompromitovať celú infraštruktúru organizácie. Viac informácií na stránke.

Spoločnosť Dell opravuje závažnú zraniteľnosť, ktorá postihuje milióny zariadení

Výskumníci zo spoločnosti SentinelLabs objavili zraniteľnosti v ovládači nachádzajúcom sa v miliónoch zariadení od spoločnosti Dell. Zraniteľnosti v ovládači existujú už od jeho prvého vydania v roku 2009. Potenciálnemu útočníkovi umožňujú eskaláciu privilégií či vykonanie kódu s oprávneniami jadra. Môžu sa nachádzať vo všetkých zariadeniach, ktoré používali obslužné programy pre aktualizáciu, ako napríklad Dell Command Update, Dell System Inventory Agent, Alienware Update či Dell Platform Tags. Viac informácií na stránke.

Microsoft opravil 55 zraniteľností, z toho 3 zero-day

Spoločnosť Microsoft vydala balík opráv Patch Tuesday, v ktorom opravila 55 zraniteľností. Z nich 50 označila ako vysoko závažné a 4 ako kritické. 3 zraniteľnosti sú typu zero-day, no zatiaľ neboli aktívne zneužívané. Väčšina najzávažnejších chýb zabezpečenia umožňuje vzdialené vykonávanie kódu, či zvýšenie oprávnení útočníka. Viac informácií na stránke.

Vo VMware vRealize Business for Cloud sa vyskytuje kritická zraniteľnosť

Spoločnosť VMware opravila kritickú zraniteľnosť vyskytujúcu sa v produkte vRealize Business for Cloud. Zneužitím tejto chyby môže dôjsť k vzdialenému vykonaniu kódu neautentifikovaným útočníkom. Viac informácií na stránke.

Kritická zraniteľnosť produktu VMware vCenter Server

Zraniteľnosť sa nachádza na serveri VMware vCenter Server. Chyba existuje z dôvodu nedostatočného overenia vstupu v doplnku vSAN Health Check, ktorý je predvolene povolený na serveri vCenter. Zraniteľnosť je možné zneužiť, ak je na serveri dostupný port 443. Potenciálny útočník so sieťovým prístupom na port 443 by mohol vykonávať ľubovoľné príkazy s neobmedzenými oprávneniami v základnom hostiteľskom operačnom systéme, ktorý je hostiteľom servera vCenter. Zároveň aktualizácia rieši aj zraniteľnosť v mechanizme autentifikácie niekoľkých doplnkov servera. Viac informácií na stránke.