Mesačný prehľad kritických zraniteľností
Júl 2024

1. Operačné systémy Microsoft Windows

Spoločnosť Microsoft opravila v mesiaci júl 4 kritické a 81 vysoko závažných zraniteľností v operačných systémoch Windows.

Kritické zraniteľnosti v komponente Windows Remote Desktop Licencing Service spočívajú v podtečení celočíselnej premennej (CVE-2024-38074) a pretečení medzipamäte haldy (CVE-2024-38076, CVE-2024-38077). Vzdialený neautentifikovaný útočník by ich prostredníctvom zaslania špeciálne vytvorených paketov alebo správ mohol zneužiť na vykonanie škodlivého kódu.

Kritická zraniteľnosť s označením CVE-2024-38060 nachádzajúca sa v komponente Windows Imaging Component spočíva v pretečení medzipamäte haldy a umožňuje vzdialené vykonanie škodlivého kódu. Úspešné zneužitie zraniteľnosti vyžaduje, aby autentifikovaný útočník nahral škodlivý súbor TIFF na zraniteľný server.

Aktívne zneužívaná zero-day zraniteľnosť v komponente Hyper-V (CVE-2024-38080) spočíva v pretečení celočíselnej premennej a vzdialený autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií na úroveň používateľa SYSTEM.

Komponent MSHTML Platform obsahuje aktívne zneužívanú zero-day zraniteľnosť s označením CVE-2024-38112, ktorú možno zneužiť na vykonanie bližšie nešpecifikovaných útokov typu spoofing. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí spustiť škodlivý súbor, ktorý vytvoril útočník.

Vysoko závažné zraniteľnosti umožňujúce vykonanie kódu sa nachádzajú v komponentoch Xbox Wireless Adapter (CVE-2024-38078), Microsoft Windows Performance Data Helper Library (CVE-2024-38019, CVE-2024-38025, CVE-2024-38028), DHCP Server Service (CVE-2024-38044), Windows Distributed Transaction Coordinator (CVE-2024-38049), Windows Layer-2 Bridge Network Driver (CVE-2024-38053), Windows Fax Service (CVE-2024-38104), Windows MultiPoint Services (CVE-2024-30013), Microsoft Xbox (CVE-2024-38032) a Windows Graphics Component (CVE-2024-38051). Zneužitie zraniteľností CVE-2024-30013, CVE-2024-38032 a CVE-2024-38051 vyžaduje interakciu zo strany používateľa.

Ostatné zraniteľnosti vysokej závažnosti umožňujú eskaláciu privilégií, zneprístupnenie služby, obídenie bezpečnostného prvku alebo získanie neoprávneného prístupu k citlivým údajom.

Zraniteľné systémy:

Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 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 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems

Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2022, 23H2 Edition (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://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

Koniec podpory pre Windows Server 2012 a Windows Server 2012 R2

Spoločnosť Microsoft plánovane zrušila podporu pre Windows Server 2012 a Windows Server 2012 R2. Po dátume 10. októbra 2023 už tieto produkty nebudú dostávať aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online.

Odporúčania:

Administrátorom a používateľom systémov Windows Server 2012 a Windows Server 2012 R2 odporúčame prejsť na novšiu verziu operačného systému alebo používať rozšírenie ESU na dobu určitú.
Viac informácií na stránke.

2. Kancelárske balíky Microsoft Office a Office Web Apps

Spoločnosť Microsoft vydala v mesiaci júl bezpečnostné aktualizácie, ktoré opravujú 3 kritické a 4 vysoko závažné zraniteľnosti v kancelárskych balíkoch Microsoft Office a Office Web Apps.

Zraniteľnosti CVE-2024-38023, CVE-2024-38024 a CVE-2024-38094 v produkte Microsoft SharePoint Server umožňujú vzdialenému autentifikovanému útočníkovi s oprávneniami úrovne „Site Owner“ alebo vyššie vykonať škodlivý kód v kontexte SharePoint servera. Zraniteľnosť je možné zneužiť nahraním špeciálne vytvoreného súboru a následným zaslaním špeciálne vytvorenej API požiadavky, ktorá vedie k deserializácii parametrov tohto súboru.

Microsoft SharePoint Server obsahuje aj zraniteľnosť s označením CVE-2024-32987, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu útokov SSRF (Server Side Request Forgery) a získanie neoprávneného prístupu k citlivým údajom.

Zraniteľnosť CVE-2024-38021 v Microsoft Outlook spočíva v nesprávnom overovaní vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom zaslania špeciálne vytvoreného odkazu mohol zneužiť na obídenie ochrany Protected View Protocol a následné vykonanie škodlivého kódu. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa, ktorý musí povoliť blokovaný obsah prijatý z externých zdrojov.

CVE-2024-38164 a CVE-2024-38176 v produkte GroupMe umožňujúce eskaláciu privilégií boli automaticky opravené spoločnosťou Microsoft a nevyžadujú dodatočnú aktualizáciu systémov.

Zraniteľné systémy:

GroupMe
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription 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
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38164
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38176
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-32987
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094

3. Internetové prehliadače

Microsoft Internet Explorer

Spoločnosť Microsoft ukončila podporu prehliadača Internet Explorer 15.6.2022 pre hlavnú líniu operačných systémov Windows 10 a 11. Spoločnosť Microsoft za mesiac máj neopravila žiadne kritické ani vysoko závažné zraniteľnosti pre zvyšné operačné systémy podporujúce Internet Explorer.

Odporúčania:

Odporúčame prestať používať a odinštalovať Internet Explorer a nahradiť ho podporovaným prehliadačom Microsoft Edge.

Zdroje:

https://msrc.microsoft.com/update-guide/en-us

Microsoft Edge

Spoločnosť Microsoft v mesiaci júl neopravila ani jednu kritickú alebo vysoko závažnú zraniteľnosť v prehliadači Microsoft Edge.

Zdroje:

https://msrc.microsoft.com/update-guide/en-us

Mozilla Firefox

Spoločnosť Mozilla v mesiaci júl opravila 4 vysoko závažné zraniteľnosti v línii internetových prehliadačov Firefox a Firefox ESR.

Zraniteľnosti s označením CVE-2024-6604 (línie Firefox a Firefox ESR) a CVE-2024-6615 (Firefox) možno zneužiť na poškodenie obsahu pamäte a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.

CVE-2024-6606 sa nachádza v komponente Clipboard, spočíva v nesprávnom overovaní indexov používaných pre prístup do polí a možno ju prostredníctvom čítania mimo povolených hodnôt zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Firefox pre Android obsahuje zraniteľnosť CVE-2024-6605, ktorá umožňuje okamžitú interakciu s výzvami o povoleniach a možno ju zneužiť na realizáciu tzv. tapjacking útokov a následnú eskaláciu privilégií.

Zneužitie všetkých zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

Zraniteľné systémy:

Mozilla Firefox verzie staršie ako 128
Mozilla Firefox ESR verzie staršej ako 115.13

Odporúčania:

Odporúčame aktualizovať Firefox na verziu 128 a Firefox ESR na verziu 115.13.

Zdroje:

https://www.mozilla.org/en-US/security/advisories/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-29/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-30/
https://exchange.xforce.ibmcloud.com/vulnerabilities/297704
https://exchange.xforce.ibmcloud.com/vulnerabilities/297718
https://exchange.xforce.ibmcloud.com/vulnerabilities/297707
https://exchange.xforce.ibmcloud.com/vulnerabilities/297706

Google Chrome

V mesiaci júl spoločnosť Google vydala bezpečnostné aktualizácie, ktoré opravili celkom 13 vysoko závažných zraniteľností.

Najzávažnejšie zraniteľnosti sa nachádzajú v komponentoch V8 (CVE-2024-6773, CVE-2024-6779), DevTools (CVE-2024-6778), Screen Capture (CVE-2024-6774), Media Stream (CVE-2024-6775), Audio (CVE-2024-6776), Navigation (CVE-2024-6777), Downloads (CVE-2024-6988), Loader (CVE-2024-6989) a Dawn(CVE-2024-6991) a umožňujú vzdialené vykonanie škodlivého kódu.

CVE-2024-7255 v komponente WebTransport spočíva v čítaní mimo povolené hodnoty a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Nedostatočné overovanie dát v komponente Dawn (CVE-2024-7256) a implementačnú chybu v komponente V8 (CVE-2024-6772) možno zneužiť na obídenie bezpečnostných mechanizmov.

Zneužitie všetkých vyššie uvedených zraniteľností vyžaduje interakciu zo strany používateľa, ktorý musí otvoriť špeciálne vytvorený webový obsah.

Zraniteľné systémy:

Google Chrome pre Windows a Mac verzie staršej ako 126.0.6478.182/183
Google Chrome pre Linux verzie staršej ako 126.0.6478.182

Odporúčania:

Odporúčame aktualizáciu prehliadača Chrome pre Windows a Mac aspoň na verziu 126.0.6478.182/183 a Linux verzie aspoň na verziu 126.0.6478.182.

Zdroje:

https://chromereleases.googleblog.com/2024
https://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_30.html
https://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
https://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/298021
https://exchange.xforce.ibmcloud.com/vulnerabilities/298017
https://exchange.xforce.ibmcloud.com/vulnerabilities/298016
https://exchange.xforce.ibmcloud.com/vulnerabilities/298018
https://exchange.xforce.ibmcloud.com/vulnerabilities/298019
https://exchange.xforce.ibmcloud.com/vulnerabilities/298020
https://exchange.xforce.ibmcloud.com/vulnerabilities/298022
https://exchange.xforce.ibmcloud.com/vulnerabilities/298023
https://exchange.xforce.ibmcloud.com/vulnerabilities/298471

https://exchange.xforce.ibmcloud.com/vulnerabilities/298473
https://exchange.xforce.ibmcloud.com/vulnerabilities/298474
https://exchange.xforce.ibmcloud.com/vulnerabilities/350205
https://exchange.xforce.ibmcloud.com/vulnerabilities/350206

4. Adobe Acrobat a Reader

V produkte Adobe Acrobat a Reader neboli v mesiaci júl opravené žiadne kritické alebo vysoko závažné zraniteľnosti.

Zdroje:

https://helpx.adobe.com/security/security-bulletin.html#acrobat

5. Frameworky

Microsoft .NET Framework

V mesiaci júl spoločnosť Microsoft opravila 4 vysoko závažné zraniteľnosti vo frameworku .NET.

CVE-2024-35264 v produktoch .NET a Visual Studio Code spočíva v použití odalokovaného miesta v pamäti, ktoré možno zneužiť na vzdialené vykonanie kódu. Pre úspešné zneužitie zraniteľnosti musí útočník vyhrať súbeh procesov, čo môže docieliť prerušením prúdu http/3 počas prebiehajúceho spracovávania tela požiadavky.

Zraniteľnosti s označením CVE-2024-30105 (.NET Core, Visual Studio) a CVE-2024-38095 (.NET, Visual Studio) spočívajú v nesprávnom overovaní vstupov a využitia dostupných zdrojov a vzdialený neautentifikovaný útočník by ich prostredníctvom zaslania špeciálne vytvorených požiadaviek mohol zneužiť na zneprístupnenie služby.

Produkty .NET, .NET Framework a Visual Studio obsahujú aj zraniteľnosť CVE-2024-38081, ktorá umožňuje eskaláciu privilégií na oprávnenia úrovne SYSTEM. Zneužitie zraniteľnosti vyžaduje interakciu zo strany lokálneho používateľa, ktorý musí spustiť špeciálne vytvorený inštalátor Visual Studio.

Zraniteľné systémy:

.NET 6.0
.NET 8.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.6/4.6.2
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://msrc.microsoft.com/update-guide/en-us
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30105
https://exchange.xforce.ibmcloud.com/vulnerabilities/295669
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35264
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38081
https://exchange.xforce.ibmcloud.com/vulnerabilities/295750
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38095
https://exchange.xforce.ibmcloud.com/vulnerabilities/295754

Oracle Java

Spoločnosť Oracle v mesiaci júl vydala bezpečnostné aktualizácie, ktoré opravujú 2 vysoko závažné bezpečnostné zraniteľnosti v rámci Oracle Java SE.

Oracle GraalVM for JDK obsahuje zraniteľnosť CVE-2024-27983, ktorá sa nachádza v externom komponente Node.js a vzdialený neautentifikovaný útočník by ju mohol zneužiť na zneprístupnenie služby a úpravu dát prístupných pre GraalVM for JDK.

CVE-2024-21147 (GraalVM for JDK, GraalVM Enterprise Edition, Java SE) nachádzajúcu sa v komponente Hotspot možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a vykonanie neoprávnených zmien v systéme. Zraniteľnosť možno zneužiť zaslaním špeciálne vytvorených dát na API rozhranie zraniteľného komponentu.

Zraniteľné systémy:

Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1
Oracle GraalVM Enterprise Edition: 20.3.14, 21.3.10
Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1

Odporúčania:

Odporúčame aktualizovať zraniteľné verzie Java SE na aktuálne verzie prostredníctvom Java Auto Update alebo na stránke spoločnosti Oracle, ktorú môžete nájsť v časti Zdroje.

Zdroje:

https://www.oracle.com/security-alerts/cpujul2024.html
https://www.oracle.com/security-alerts/cpujul2024verbose.html#JAVA

6. Iné závažné zraniteľnosti

Kritická zraniteľnosť v Docker Engine

Vývojári kontajnerizačnej technológie Docker Engine vydali bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť. CVE-2024-41110 možno zneužiť na obídenie autorizačných

pluginov AuthZ a eskaláciu privilégií. Jedná sa o opätovný výskyt zraniteľnosti odstránenej v januári 2019, ktorej oprava nebola zakomponovaná do novších verzií Docker Engine 19.03 a vyššie. **Viac informácií na stránke.**

Zraniteľnosti v serveroch Atlassian

Spoločnosť Atlassian vydala bezpečnostné aktualizácie svojich produktov Bamboo Data Center a Server, Confluence Data Center a Server, Jira Data Center and Server a Jira Service Management Data Center a Server, ktoré opravujú 30 zraniteľností. Najzávažnejšie zraniteľnosti nachádzajúce sa v Bamboo Data Center a Server možno zneužiť na realizáciu SSRF útokov, vzdialené vykonanie lokálnych súborov a získanie neoprávneného prístupu do systému. Ostatné zraniteľnosti možno zneužiť na zneprístupnenie služby, získanie neoprávneného prístupu do systému alebo vykonanie neoprávnených zmien v systéme. **Viac informácií na stránke.**

Kritické zraniteľnosti v produktoch SolarWinds Access Rights Manager

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie produktu SolarWinds Access Rights Manager, ktoré opravujú 13 zraniteľností, z toho 8 označených ako kritické. Kritické zraniteľnosti možno zneužiť na vykonanie škodlivého kódu a získanie úplnej kontroly nad systémom. Ostatné zranite--ľnosti umožňujú neoprávnený prístup do systému, neoprávnený prístup k citlivým údajom a vykonanie neoprávnených zmien v systéme. **Viac informácií na stránke.**

Kritické zraniteľnosti v produktoch Cisco Security Email Gateway a Cisco Smart Software Manager On-Prem

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch Cisco Secure Email Gateway a Cisco Smart Software Manager On-Prem. Zraniteľnosti v označením CVE-2024-20401 a CVE-2024-20419 by vzdialený útočník mohol zneužiť na modifikáciu súborov na súborovom systéme zariadení a získanie neoprávneného prístupu do systému. **Viac informácií na stránke.**

Kritická zraniteľnosť servera Exim

Mailový server Exim obsahuje zraniteľnosť, ktorá umožňuje útočníkom doručiť obetiam do mailboxu súbory so zakázanou príponou. Ochranou servera prejdú aj škodlivé spustiteľné súbory. **Viac informácií na stránke.**

Kritická bezpečnostná zraniteľnosť v OpenSSH

Vývojári nástroja OpenSSH vydali bezpečnostnú aktualizáciu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť. Zraniteľnosť možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad zraniteľným systémom. Bezpečnostní výskumníci počas jej detailnej analýzy odhalili aj jej menej závažný variant CVE-2024-6387 s označením CVE-2024-6409, ktorý taktiež možno zneužiť na vykonanie kódu. **Viac informácií na stránke.**

Citrix opravila viacero zraniteľností svojich produktov

Spoločnosť Citrix opravila kritické a vysoko závažné zraniteľnosti vo viacerých svojich produktoch. Zraniteľnosti umožňujú útočníkom získať privilégiá na úrovni SYSTEM, presmerovať používateľov na škodlivé webstránky, získať citlivé údaje alebo spôsobiť nedostupnosť systému. **Viac informácií na stránke.**

Vysoko závažné zraniteľnosti SAP

Spoločnosť SAP vydala v júli 2024 balík opráv pre svoje produkty opravujúcich 16 zraniteľností v aplikáciách PDCE, Commerce, Landscape Management, Document Builder, NetWeaver Knowledge Management XMLEditor a ďalších. 2 z nich sú označené ako vysoko závažné. Úspešné zneužitie umožňuje neautentifikovanému útočníkovi čítať všeobecné údaje z tabuľky alebo pristupovať k nesprávne nakonfigurovaným stránkam. Na zraniteľnosť upozornila spoločnosť Onapsis Research Labs (ORL). **Viac informácií na stránke.**

Microsoft v rámci júlového Patch Tuesday opravil kritické a zero-day zraniteľnosti

Spoločnosť Microsoft vydala v júli 2024 balík opráv pre portfólio svojich produktov opravujúci 139 zraniteľností, z ktorých 54 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v produkte Microsoft SharePoint Server a komponentoch Windows Imaging Component a Windows Remote Desktop Licensing Service. Zero-day zraniteľnosti s označením CVE-2024-38080 a CVE-2024-38112 sú aktívne zneužívané útočníkmi. **Viac informácií na stránke.**

Kritická zraniteľnosť protokolu RADIUS

Tím výskumníkov popísal útok na protokol RADIUS, ktorým môže útočník pomocou manipulácie prefixu paketu a vytvorením kolízie MD5 pre premennú v ňom zakomponovanú získať povolenie na prístup do administrátorského rozhrania sieťového zariadenia. Útočník nepotrebuje poznať heslo ani zdieľané tajomstvá. **Viac informácií na stránke.**

Aktívne zneužívaná zero-day zraniteľnosť v prepínačoch CISCO NEXUS a MDS

Spoločnosť CISCO vydala bezpečnostné aktualizácie na sieťové prepínače série NEXUS a MDS, ktoré opravujú aktívne zneužívanú zero-day zraniteľnosť umožňujúcu vykonanie škodlivého kódu. Napriek tomu, že zneužitie zraniteľnosti vyžaduje administrátorský prístup k zraniteľnému zariadeniu, CISCO a bezpečnostní výskumníci zo spoločnosti SYGNIA evidujú prípady jej úspešného zneužitia zo strany čínskej skupiny VELVET ANT. **Viac informácií na stránke.**