Mesačný prehľad kritických zraniteľností
Apríl 2018

1. Operačné systémy Microsoft Windows

V apríli spoločnosť Microsoft opravila 6 kritických zraniteľností operačného systému Microsoft Windows.

Vzdialené spustenie škodlivého kódu umožňujú zraniteľnosti CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1015 a CVE-2018-1016. Všetky sú spôsobené tým, že knižnica fontov operačného systému Windows nesprávne spracováva špeciálne vytvorené písma. Útočník na ich zneužitie potrebuje aj interakciu používateľa. Útočník môže vytvoriť špeciálnu stránku, využívajúcu tieto zraniteľnosti, ale musí presvedčiť používateľa, aby túto stránku navštívil. To sa zvyčajne snaží dosiahnuť tým, že používateľa presvedčí, aby klikol na odkaz v e-maile, ktorý ho privedie na danú stránku. Ďalšou možnosťou zneužitia je zdieľanie špeciálne vytvoreného súboru využívajúceho jednu z týchto zraniteľností. Využitie zraniteľností v tomto prípade je možné iba ak používateľ súbor otvorí. Pri úspešnom zneužití niektorej z týchto zraniteľností by útočník mohol získať práva práve prihláseného používateľa. To znamená, že ak bol používateľ administrátorom, útočník môže inštalovať programy, zobraziť, zmeniť alebo vymazať údaje či vytvárať nové plnohodnotné účty. Teda používateľa s nižšími právami ako administrátorskými, sú menej ovplyvnené týmito zraniteľnosťami.

Zraniteľnosť CVE-2018-0986 popísaná aj v našom varovaní taktiež umožňuje útočníkovi vzdialené spustenie akéhokoľvek kódu. Je to spôsobené tým, že Microsoft Malware Protection Engine nesprávne skenuje špeciálne vytvorený súbor a spôsobí poškodenie pamäte. Na zneužitie tejto zraniteľnosti musí teda Microsoft Malware Protection Engine verzie s touto zraniteľnosťou preskenovať špeciálne vytvorený súbor. To znamená, že útočník musí dostať súbor na miesto, kde Microsoft Malware Protection Engine skenuje. Útočník môže použiť webovú stránku na to, aby dostal súbor do systému používateľa. Ďalšími spôsobmi je dostať súbor k používateľovi pomocou e-mailu alebo okamžitej správy. Útočník by mohol využiť aj webové stránky, ktoré prijímajú alebo zdieľajú obsah poskytovaný používateľom a nahrajú súbor na zdieľané miesto. Súbor sa potom preskenuje pomocou Microsoft Malware Protection Engine, ktorý beží na hostiteľskom serveri. Pri úspešnom zneužití tejto zraniteľnosti je možné spúšťať akýkoľvek kód v kontexte účtu LocalSystem a tak prevziať kontrolu nad systémom. Tým môže útočník získať vyššie práva, čo mu umožní inštalovať programy, zobrazovať, meniť alebo mazať údaje alebo vytvárať plnohodnotné účty.

Ak je zapnutá ochrana príslušným antimalware systémom v reálnom čase, tak sa programom Microsoft Malware Protection Engine skenujú súbory automaticky, čo vedie k zneužitiu zraniteľnosti. Ak je ochrana v reálnom čase vypnutá, útočník musí počkať, kým sa vykoná naplánované skenovanie, aby mohol využiť túto zraniteľnosť.

Program Microsoft Malware Protection Engine má zabudovaný mechanizmus automatického zisťovania a zavádzania aktualizácií, takže nie je potrebné vykonávať aktualizáciu ručne administrátorom alebo koncovým používateľom. Aktualizácia by sa mala uplatniť do 48 hodín od jej zverejnenia, pričom daný čas závisí od použitého softvéru, pripojenia k internetu a konfigurácie infraštruktúry.

Poslednou kritickou zraniteľnosťou opravenou tento mesiac je zraniteľnosť CVE-2018-1004, ktorá taktiež umožňuje vzdialené spúšťanie ľubovoľného kódu. Je spôsobená tým, ako stroj VBScript spracováva objekty v pamäti. Jej zneužitím sa pamäť poškodí takým spôsobom, že umožní útočníkovi spúšťať ľubovoľný kód ako práve prihlásený používateľ. Zneužitie je možné pomocou špeciálne vytvorenej webovej stránky, ktorá túto zraniteľnosť využije. Útočník môže poslať používateľovi odkaz na stránku pomocou e-mailu, pričom sa zraniteľnosť využije až po prezretí stránky. Útočník môže taktiež vložiť ovládací prvok ActiveX označený ako bezpečný na inicializáciu do dokumentu Microsoft Office a tým zneužiť zraniteľnosť. Úspešné zneužitie zraniteľnosti umožní útočníkovi získať práva práve prihláseného používateľa.

Zraniteľné systémy:

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 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 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, version 1709 (Server Core installation)
Microsoft Exchange Server 2013
Microsoft Exchange Server 2016
Microsoft Forefront Endpoint Protection 2010
Microsoft Security Essentials
Microsoft System Center 2012 Endpoint Protection
Windows Intune Endpoint Protection

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-0986
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1004
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1010
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1012
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1013
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1015
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1016

2. Kancelárske balíky Microsoft Office a Office Web Apps

Závažné zraniteľnosti CVE-2018-0920, CVE-2018-1011, CVE-2018-1026, CVE-2018-1027, CVE-2018-1028, CVE-2018-1029 a CVE-2018-1030 umožňujú útočníkovi spúšťať kód na diaľku. Zraniteľnosti sú spôsobené nesprávnym narábaním s objektmi v pamäti a nesprávnym spracovávaním špeciálne upravených fontov. Na zneužitie niektorej z týchto zraniteľností môže útočník použiť špeciálne vytvorenú stránku. Útočník však musí presvedčiť používateľa, aby stránku otvoril, čo môže urobiť tak, že ho presvedčí, aby klikol na odkaz v e-maile alebo okamžitej správe. Prípadne by mohol útočník využiť aj špeciálne vytvorený súbor navrhnutý na zneužitie zraniteľnosti. Aj v tomto prípade však musí útočník presvedčiť používateľa, aby otvoril súbor. Pri úspešnom zneužití niektorej z týchto zraniteľností, môže prevziať kontrolu nad systémom. V takom prípade môže inštalovať programy, zobrazovať, meniť alebo mazať dáta či vytvárať plnohodnotné účty.

Zraniteľnosť CVE-2018-0950 spôsobujúca únik citlivých informácií je bližšie popísaná v našom varovaní.

CVE-2018-1007 taktiež spôsobuje únik informácií. Nastáva, keď Microsoft Office nesprávne zverejňuje obsah svojej pamäte. Útočník musí vytvoriť špeciálny súbor, a presvedčiť používateľa, aby ho otvoril. Okrem toho, musí útočník poznať miesto adresy pamäte, kde bol objekt vytvorený. Po úspešnom zneužití získa útočník informácie, ktoré môže ďalej použiť na ohrozenie počítača alebo údajov používateľa.

Zraniteľnosti CVE-2018-1005, CVE-2018-1014 a CVE-2018-1032 môžu spôsobiť zvýšenie práv, tým, že Microsoft SharePoint Server nesprávne spracuje špeciálne vytvorenú webovú požiadavku na SharePoint Server. Útočník túto zraniteľnosť môže zneužiť poslaním špeciálne upravenej URL adresy používateľovi zasiahnutého SharePoint servera. Po úspešnom zneužití zraniteľnosti CVE-2018-1005 alebo CVE-2018-1032 môže útočník vykonať cross-site scripting útoky na zraniteľných systémoch a spúšťať skripty ako práve prihlásený používateľ. To môže

útočníkovi umožniť čítať obsah, na ktorý nemá právo, vykonávať akcie v službe SharePoint ako daný používateľ (napríklad zmena alebo odstránenie obsahu či vložiť škodlivý obsah do prehliadača používateľa).
Po zneužití CVE-2018-1014 má útočník možnosť presmerovať používateľov, ktorí sa pokúšajú pristúpiť k obsahu Silverlight na zraniteľnom serveri SharePoint na útočníkom vytvorený škodlivý obsah. Zneužiť túto zraniteľnosť je možné iba ak používateľ ešte nemá nainštalovaný Silverlight, a klikne na útočníkom upravenú URL adresu a následne klikne na odkaz na stiahnutie Silverlight na stránke SharePoint.

Zraniteľné systémy:

Microsoft Project Server 2013 Service Pack 1
Microsoft Project Server 2010 Service Pack 2
Microsoft SharePoint Enterprise Server 2016
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Office Word Viewer
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2016 Click-to-run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-run (C2R) for 64-bit editions
Microsoft Office 2016 for Mac
Microsoft Office Online Server 2016
Microsoft Office Web Apps 2010 Service Pack 2
Microsoft Office Web Apps 2013 Service Pack 1
Microsoft Excel 2010 Service Pack 2 (32-bit editions)
Microsoft Excel 2010 Service Pack 2 (64-bit editions)
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 Excel 2007 Service Pack 3

Odporúčania:

Vzhľadom množstvo závažných zraniteľností odporúčame bezodkladne 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://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=164
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0920
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0950
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1011

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1014
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1005
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1007
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1026
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1027
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1028
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1029
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1030
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1032

3. Internetové prehliadače

Microsoft Internet Explorer

V rámci aprílového balíka opráv boli spoločnosťou Microsoft vydané opravy 8 kritických zraniteľností.
Zraniteľnosti CVE-2018-0870, CVE-2018-0991, CVE-2018-1018 a CVE-2018-1020 umožňujú útočníkovi spustiť ľubovoľný kód na diaľku. Všetky tri zraniteľnosti sú spôsobené nesprávnym pristupovaním k objektom v pamäti, čo môže dať útočníkovi možnosť spúšťať ľubovoľný kód ako práve prihlásený používateľ. Útočník môže zneužiť túto zraniteľnosť tak, že vytvorí špeciálnu webovú stránku, a presvedčí používateľa aby tú stránku navštívil. Taktiež by na zneužitie mohol využiť stránky, ktoré akceptujú alebo obsahujú reklamy poskytované používateľmi a to pridaním špeciálne vytvoreného obsahu. V každom prípade musí útočník na zneužitie zraniteľnosti presvedčiť používateľa, aby navštívil stránku. To môže dosiahnuť poslaním odkazu na stránku pomocou e-mailu alebo okamžitej správy. Pri úspešnom zneužití útočník získa práva prihláseného používateľa. Ak bol používateľom administrátor, útočník môže inštalovať programy, zobraziť, meniť alebo mazať údaje a vytvárať plnohodnotné účty.
Zraniteľnosti CVE-2018-0996 a CVE-2018-0988 sú spôsobené tým, ako skriptovací engine narába s objektmi v pamäti. Dopady a využitie týchto zraniteľností sú veľmi podobné ako pri zraniteľnostiach spomínaných vyššie. Rozdielom je, že tieto dve zraniteľnosti môže útočník zneužiť aj tým, že vloží ovládací prvok ActiveX označený ako bezpečný na inicializáciu do dokumentu Microsoft Office.
Zraniteľnosti CVE-2018-0981 a CVE-2018-1000 spôsobujú únik informácií. Je to taktiež spôsobené tým, ako skriptovací engine narába s objektmi v pamäti. Pamäť sa môže poškodiť takým spôsobom, že útočník získa informácie, ktoré môže použiť na ďalšie zneužitie používateľovho počítača alebo jeho dát. Zraniteľnosti sa dajú zneužiť podobnými spôsobmi ako bolo spomínané vyššie.

Zraniteľné systémy:

Microsoft Internet Explorer 11 v systémoch Windows 10 verzií 1511,1607, 1703, 1709 pre 32 aj 64 bitových verziách
Microsoft internet Explorer 11 v systémoch Windows 7 pre 32 aj 64 bitové verzie
Microsoft internet Explorer 11 v systéme Windows 8.1 pre 32 aj 64 bitové verzie
Microsoft internet Explorer 11 v systéme Windows Server 2008 R2 pre 64 bitové verzie Service Pack 1
Microsoft internet Explorer 11 v systémoch Windows Server 2012 R2

Microsoft internet Explorer 11 v systémoch Windows 7 pre 32 aj 64 bitové verzie
Microsoft Internet Explorer 10 pre systém Windows Server 2012
Microsoft internet Explorer 9 v systémoch Windows Server 2008 pre 32 aj 64 bitové verzie Service Pack 2

Odporúčania:

Vzhľadom množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-1018
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0996
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0981
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1000
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0870
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0988
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0991
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1020

Microsoft Edge

V apríli bola zverejnená aktualizácia, ktorá opravuje viacero kritických zraniteľností umožňujúcich vykonať škodlivý kód na diaľku.
Všetky aprílové kritické zraniteľnosti umožňujú útočníkovi spustiť ľubovoľný kód, keďže skriptovací engine nesprávne narába s objektmi v pamäti. Zneužitie je možné len za pomoci používateľa, ktorého musí útočník presvedčiť, aby navštívil jeho špeciálne vytvorenú stránku. Úspešné zneužitie týchto zraniteľností umožňuje útočníkovi prebrať kontrolu nad systémom a vykonať ľubovoľný škodlivý kód s oprávneniami práve prihláseného používateľa. V prípade, že používateľ mal administrátorské práva útočník získa možnosť inštalovať programy, prezerať, meniť a mazať dáta, prípadne vytvárať plnohodnotné používateľské účty.

Zraniteľné systémy:

Microsoft Edge v systémoch Windows 10 verzií 1511, 1607, 1703 a 1709 a 32-bitových aj 64-bitových verziách
Microsoft Edge v systéme Windows Server 2016

Odporúčania:

Vzhľadom na množstvo kritických zraniteľností odporúčame bezodkladne 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-2018-0979
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0980
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0990
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0993
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0994
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0995
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1019
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1023

Mozilla Firefox

Spoločnosť Mozilla v mesiaci apríl nevydala opravy žiadnych zraniteľností.

Zdroje:

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

Google Chrome

Spoločnosť Google vydala aktualizácie prehliadača Chrome, ktoré obsahujú opravy 33 bezpečnostných zraniteľností. Z toho 2 kritické a 6 závažných zraniteľnosti.

Odporúčania:

Odporúčame overiť, či sa prehliadač Chrome automaticky aktualizoval na verziu 66.0.3359.117, prípadne novšiu. V prípade potreby odporúčame aplikovať aktualizáciu ručne cez menu otvorením okna s aktuálne nainštalovanou verziou, čo zároveň spustí aj kontrolu dostupnosti aktualizácie.

Zdroje:

https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html

4. Adobe Flash Player

Tento mesiac boli vydané aktualizácie na tri kritické zraniteľnosti CVE-2018-4932, CVE-2018-4935 a CVE-2018-4937 v Adobe Flash Playeri verzie 29.0.0.113 a starších. Tieto zraniteľnosti môžu spôsobiť spustenie kódu ako práve prihlásený používateľ. Okrem toho boli tento mesiac opravené aj dve závažné zraniteľnosti, ktoré môžu spôsobiť únik informácií.

Zraniteľné systémy:

Adobe Flash Player Desktop Runtime 29.0.0.113 a staršie
Adobe Flash Player pre Google Chrome 29.0.0.113 a staršie
Adobe Flash Player pre Microsoft Edge a Internet Explorer 29.0.0.113 a staršie

Odporúčania:

Používateľom odporúčame čo najskôr aktualizovať zraniteľné systémy. Jedná sa najmä o Adobe Flash Player, ktorý treba aktualizovať na verziu 29.0.0.140. 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/apsb18-08.html

5. Frameworky

Microsoft .NET Framework

Pre Microsoft .NET Framework neboli v apríli vydané žiadne aktualizácie.

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

Oracle Java

Spoločnosť Oracle vydala v mesiaci apríl veľkú sadu aktualizácií a opravuje tak 14 zraniteľností pre Oracle Java SE. Väčšina týchto zraniteľností sa dá využiť vzdialene bez overenia, čo znamená, že môžu byť zneužité pomocou siete bez vyžiadania užívateľského mena a hesla. Za predpokladu, že používateľ Java appletu alebo Java Web Start má administrátorské práva (typické pre operačný systém Windows) majú tieto zraniteľnosti omnoho horší dopad ako keď používateľ nemá oprávnenia administrátora (typické pre operačný systém Linux).

Zraniteľné systémy:
Java SE 10
Java SE 6u181, 7u171, 8u162
Java SE Embedded 8u152, 8u161
JRockit R28.3.17

Odporúčania:
Vzhľadom na závažnosť uvedených zraniteľností odporúčame čo najskôr aktualizovať zraniteľné verzie Java SE a Java SE Embedded na aktuálne verzie, t.j. Java SE 8u171, Java 10.0.1 a Java SE Embedded 8u171, prostredníctvom Java Auto Update, alebo na stránke spoločnosti Oracle, viď prvý odkaz v zdrojoch.

Zdroje:
http://www.oracle.com/technetwork/indexes/downloads/index.html#java
http://www.oracle.com/technetwork/topics/security/alerts-086861.html
http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html

6. Iné závažné zraniteľnosti

MySQL Server v Juniper Junos Space

Zraniteľnosť CVE-2014-3413 môže spôsobiť únik citlivých údajov prípadne môže umožniť útočníkovi získať kontrolu nad systémom. Viac informácií o tejto zraniteľnosti môžete získať v našom varovaní.

Zraniteľné systémy:
Juniper Junos verzie staršej ako 13.3R1.8

Odporúčania:
Zraniteľnosť je v tomto čase už opravená, takže odporúčame urýchlene aktualizovať na verziu 13.3R1.8.

Zdroje:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=162
https://nvd.nist.gov/vuln/detail/CVE-2014-3413
https://www.tenable.com/security/research/tra-2014-01
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10627

Redakčný systém Drupal

V redakčnom systéme Drupal boli objavené zraniteľnosti vo Form API. Na jednu z týchto zraniteľností bol zverejnený funkčný kód využívajúci danú zraniteľnosť. Zraniteľnosti sú popísané v našich dvoch varovaniach (varovanie ku CVE-2018-7600, varovanie ku CVE-2018-7602).

Zraniteľné systémy:
Drupal 6
Drupal 7 s nižšou verziou ako 7.59
Drupal 8.5 s nižšou verziou ako 8.5.3
Drupal 8.4 s nižšou verziou ako 8.4.8
Drupal 8 s nižšou verziou ako vyššie spomenuté

Odporúčania:
Odporúča sa urýchlene aktualizovať svoj redakčný softvér, alebo použiť záplaty zverejnené na prvom odkaze v zdrojoch.

Zdroje:
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=165
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=166
https://www.drupal.org/sa-core-2018-002
https://www.bleepingcomputer.com/news/security/exploitation-of-drupalgeddon2-flaw-starts-after-publication-of-poc-code/
https://research.checkpoint.com/uncovering-drupalgeddon-2/
https://thehackernews.com/2018/04/drupalgeddon3-exploit-code.html
https://www.incapsula.com/blog/this-just-in-third-critical-drupal-flaw-discovered.html

Cisco Smart Install

V zariadeniach používajúcich Smart Install Client bola nájdená zraniteľnosť umožňujúca vykonať ľubovoľný kód. Viac informácií môžete získať v našom varovaní.

Zraniteľné systémy:
Potenciálne všetky zariadenia používajúce Smart Install Client:
Catalyst 4500 Supervisor Engines
Catalyst 3850 Series
Catalyst 3750 Series
Catalyst 3650 Series
Catalyst 3560 Series

Catalyst 2975 Series
Catalyst 2960 Series
IE 2000
IE 3000
IE 3010
IE 4000
IE 4010
IE 5000
ME 3400 series
SM-ES2 SKUs
SM-ES3 SKUs
SN-X-ES3 SKUs
Na zistenie, či je Vaša verzia softvéru zraniteľná, môžete použiť Cisco IOS Software Checker.

Odporúčania:

Bola vydaná aktualizácia, ktorá túto zraniteľnosť opravuje. Odporúčaný postup pre zmiernenie dopadov môžete taktiež nájsť v našom varovaní.

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=163
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

Citrix XenServer

Našlo sa viacej zraniteľností, ktoré môžu narušiť dostupnosť systému Citrix XenServer. Ďalšie zraniteľnosti je možné využiť na vzdialené vykonanie kódu. O týchto zraniteľnostiach sa môžete dozvedieť viac v našom varovaní.

Zraniteľné systémy:

Citrix XenServer verzie staršej ako 7.4

Odporúčania:

K týmto zraniteľnostiam sú vydané záplaty, ktoré je možné najsť na prvom linku v zdrojoch. Z dôvodu závažnosti týchto zraniteľností odporúčame čím skôr nainštalovať tieto záplaty.

Zdroje:

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=161
https://support.citrix.com/article/CTX232096
https://support.citrix.com/article/CTX232655