CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 14.04.2020 г.

Съдържание

Oracle се справя с 405 бъга в своето априлско тримесечно обновяване на пачовете

13 април 2020

Администраторите на Oracle започват кампания за актуализация на критични уязвимости, която включва пускането на 405 пача.

Бизнес софтуерният гигант Oracle Corp. разкри, че 286 от тези уязвимости могат да се използват отдалечено в близо две десетки продуктови линии.

Оценени с тежест 9,8 по CVSS са 13 ключови продукта на Oracle, включително приложения за финансови услуги на Oracle, Oracle MySQL, приложения за продажба на дребно на Oracle и инструменти за поддръжка на Oracle.

Всеки от бъговете ще бъде адресиран от съвети за смекчаване или пачове от Oracle, съвпадащи с версията на корекции на Patch Tuesday на Microsoft за април.

Fusion Middleware на Oracle има 49 уязвимости, които могат да бъдат отдалечено експлоатирани без удостоверяване, т.е. могат да бъдат експлоатирани в мрежа, без да се изискват идентификационни данни на потребителя.

Общо казано, семейството софтуер Fusion Middleware има 56 нови пача, засягащи близо 20 свързани услуги, включително Identity Manager Connector (v. 9.0), Big Data Discovery (v. 1.6) и WebCenter Portal (ст. 11.1.1.9). 0, 12.2.1.3.0, 12.2.1.4.0).

Актуализациите включват и недостатъци със средна тежест за Java платформата, стандартно издание (Java SE), използвана за разработване и внедряване на Java приложения. Петнадесет бъга с тежест 8,5 по CVSS могат да бъдат експлоатирани отдалечено от неоторизиран нападател по мрежата - не се изискват потребителски идентификационни данни.

Подробности за бъговете в Java SE, заедно с техническа информация и насоки за смекчаване на всички 405 недостатъка, ще бъдат налични във вторник, 21 април 2020 г.

Oracle коригира и 34 критични уязвимости в пакета за приложения на Oracle - Financial Services, като 14 от тях са за отдалечена експлоатация. Бяха идентифицирани четиридесет и пет грешки в Oracle MySQL, като девет от тях са за отдалечено експлоатиране с тежест на CVSS от 9,8.

Популярната линия Database Server на Oracle има само девет бъга в сигурността, два са за отдалечена експлоатация и имат CVSS рейтинг 8,0. Както при много други продукти на Oracle, засегнати от недостатъци през това тримесечие, Oracle заяви, че нито един от бъговете в сървъра на база данни не е „приложим за инсталации само за клиент, т.е. за инсталации, при които няма инсталиран сървър с база данни на Oracle.“

За повече информация:

https://threatpost.com/oracle-tackles-405-bugs-for-april-quarterly-patch-update/154737/

Хакери атакуват здравни заведения с ransomware по време на пандемията от коронавирус

14 април 2020

Тъй като болниците по света се борят да отговорят на коронавирусната криза, киберпрестъпниците - без съвест и съпричастност - непрекъснато се насочват към здравни организации, изследователски центрове и други правителствени организации с цел заразяване с ransomware или с цел кражба на данни.

Атаките бяха открити между 24 и 26 март и бяха инициирани като част от фишинг кампаниите с коронавирус, които станаха широко разпространени през последните месеци.

Предоставяне на Ransomware чрез използване на CVE-2012-0158

Според изследователи кампанията е започнала със злонамерени имейли, изпращани от измамен адрес, имитиращ този на Световната здравна организация (noreply @ who.Int), изпратени до редица лица, свързани със здравната организация.

Измамните имейли съдържат документ с Rich Text Format (RTF), наречен „20200323-sitrep-63-covid-19.doc“, който при отваряне се опитва да извлече EDA2 ransomware чрез използване на известна уязвимост (CVE-2012-0158) в контролите на ListView / TreeView ActiveX на Microsoft в библиотеката MSCOMCTL.OCX.

Интересно е да се отбележи, че въпреки че името на файла ясно посочва конкретна дата (23 март 2020 г.), то не е актуализирано в хода на кампанията, за да отразява текущите дати, отбелязват изследователите на Palo Alto Networks.

Интересно е също, че авторите на злонамерен софтуер не са се постарали да направят примамките си да изглеждат истински, от първата страница на документа става ясно, че нещо не е наред.

След изпълнение, този ransomware се свързва със сървъра за командване и контрол (C2), за да изтегли изображение, което служи като главно известие за заразяване с рансъмуер на устройството на жертвата, и впоследствие предава подробности за хоста, за да създаде персонализиран ключ за криптиране на файловете на работния плот на системата с разширение ".locked20".

Освен получаване на ключа, заразеният хост използва HTTP Post заявка, за да изпрати дешифриращия ключ, криптиран с помощта на AES, на C2 сървъра.

От Palo Alto Networks са установили, че щамът ransomware е EDA2. EDA2 и Hidden Tear се считат за едни от първите видове ransomware с отворен код, които са създадени с образователни цели, но оттогава с тях са злоупотребили много хакери.

Атаките с ransomware са следствие от увеличаване на други кибератаки, свързани с пандемията. Те включват набор от фишинг имейли, които се опитват да използват кризата, за да убедят хората да кликнат върху връзки, които изтеглят malware или ransomware на техните компютри.

Тъй като болниците са подложени на ограничения във времето и натиск поради продължаващата пандемия, хакерите разчитат на организациите да платят откуп, за да възстановят достъпа до критични системи и да предотвратят нарушаване на грижите за пациентите.

Доклад, публикуван от RisKIQ миналата седмица, установява, че нападенията и злоупотребите срещу медицински заведения са нараснали с 35% между 2016 и 2019 г.,

като средният размер на искания откуп е 59 000 долара при 127 инцидента. Хакерите са предпочели предимно малки болници и здравни центрове.

Скокът в нападенията и злоупотребите срещу медицинския сектор предизвикват Интерпол да издаде предупреждение за заплахата за страните-членки.

"Киберпрестъпниците използват ransomware, за да превръщат болници и медицински услуги в цифрови заложници, като им пречат да имат достъп до жизненоважни файлове и системи, докато откупът не бъде платен", съобщават от агенцията.

За да защитят системите си от подобни атаки, Интерпол предупреди организациите освен да съхраняват данните офлайн или в друга мрежа, да внимават и за опитите за фишинг, да криптират чувствителните данни и да извършват периодично архивиране.

За повече информация:

https://thehackernews.com/2020/04/ransomware-hospitals-coronavirus.html

Microsoft и Google забавят промяната в онлайн удостоверяването

14 април 2020

COVID-19 постави реалността в момент на задържане за всички и това включва и екипите за сигурност. И Microsoft, и Google отложиха промяна, която би наложила по-добра сигурност на приложенията, която изключва несигурен протокол за достъп, наречен Basic Authentication.

Определен в RFC 2617, Basic Authentication е метод за логване в приложения за онлайн услуги с помощта на обикновена комбинация от потребителско име и парола, изпратена в HTTP header. Можете да го използвате, ако искате софтуерът за производителност на вашия компютър да се синхронизира например с вашия облачен календар или с услуга за електронна поща, вместо да осъществявате достъп до уеб приложение ръчно чрез браузъра.

Основното удостоверяване е удобно, тъй като не се нуждае от разработчици да кодират бисквитките или да обработват страниците за вход. Вместо това, то просто изпраща отново идентификационните данни с всяка HTTP заявка. Но е несигурно, защото не криптира идентификационните данни за вход.

Вместо това използва Base64 кодиране, което просто превежда двоичното съдържание в текст. Можете да преодолеете този проблем с помощта на TLS-защитена HTTPS връзка, но това все още затруднява прилагането на многофакторна автентификация (MFA).

Компаниите постепенно заменят този метод с по-модерни протоколи. Microsoft и Google преминават към OAuth 2.0, който използва токъни за удостоверяване на приложенията за онлайн услуги и им задава дата на изтичане. По този начин приложението остава разрешено за предварително определен период, като се свежда до минимум необходимостта от обмен на идентификационни данни. Също така се улеснява прилагането на многофакторната автентификация (MFA).

Microsoft обяви, че ще изключи Basic Authentication в своя Exchange Web Services (EWS) API за Office 365 още през юли 2018 г. Компанията планираше да изключи изцяло поддръжката на функцията на 13 октомври 2021 г.

В същото време компанията съветва разработчиците да започнат да се отдалечават от това API и вместо това да използват Microsoft Graph, който е по-ново API за достъп до бек-клауд облачни услуги като Exchange Online. Освен това Microsoft разшири тези свои планове през септември 2019 г., като обяви, че ще изключи основното удостоверяване в Exchange Online за Exchange ActiveSync (EAS), POP, IMAP и отдалечен PowerShell.

Google също се ангажира да изключи основното удостоверяване. През декември 2019 г. компанията предупреди, че ще откаже достъп на „по-малко защитени приложения“ до своите услуги, като предпочита OAuth 2.0. Това трябваше да се случи на 15 юни 2020 г.

Сега и двете компании леко промениха плановете си, за да дадат на своите онлайн потребители повече свобода на действие, докато се справят с хаоса около COVID-19. Microsoft заяви на 3 април, че ще отложи основното удостоверяване за Exchange Online за тези ползватели, които го използват, и засега няма да го изключи до втората половина на 2021 г.

Компанията обаче няма да промени някои от другите си планове. Тя все пак ще деактивира Basic Authentication за нови акаунти и ще продължи да разгръща поддръжката на OAuth за POP, IMAP, SMTP AUTH и Remote PowerShell.

Google също обяви в края на март, че ще отложи изключване на основната автентификация засега. Това обаче не означава, че компаниите не трябва да преминават към по-сигурни методи.

Въпреки тези корекции във времето, Google не препоръчва използването на което и да е приложение, което не поддържа OAuth. Препоръчваме ви да преминете към използване на OAuth удостоверяване, ако това е възможно за вашата организация.

И двете компании взеха други мерки в отговор на кризата със здравето. Те отлагат края на поддръжката за TLS 1.0 в съответните си браузъри, като Microsoft специално посочва COVID-19 като фактор в своето решение.

За повече информация:

https://nakedsecurity.sophos.com/2020/04/14/microsoft-and-google-delay-online-authentication-change/