CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

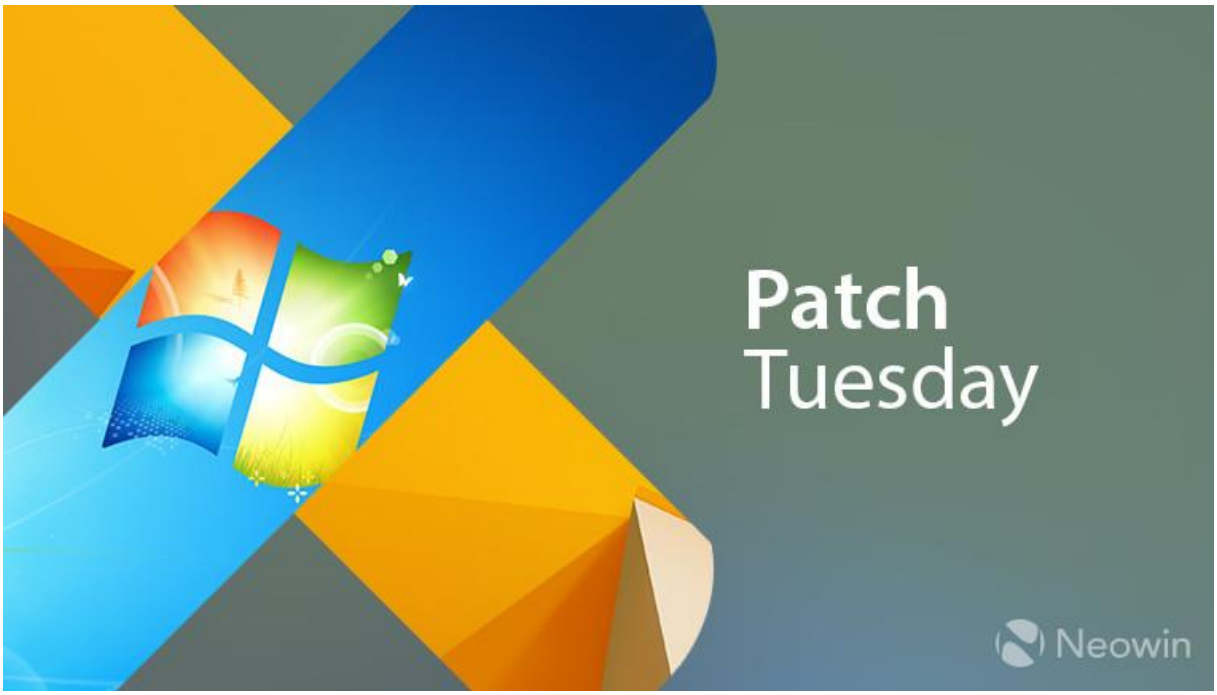
Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 16.09.2020 г.

Съдържание

Microsoft Patch вторник, септември 2020 г.

8 септември 2020 г.



Microsoft пусна актуализации за отстраняване на почти 130 уязвимости в сигурността на своята операционна система Windows и в поддържания софтуер. За нито един от недостатъците не се знае, че в момента е в активна експлоатация, но 23 от тях могат да бъдат използвани от злонамерен софтуер или недобро съдържание, за да се поеме пълен контрол на компютрите с Windows с малко или никаква помощ от потребителите.

По-голямата част от най-опасните или „критични“ грешки се занимават с проблеми в различните операционни системи Windows на Microsoft и нейните уеб браузъри, Internet Explorer и Edge. Септември е седмият пореден месец, в който Microsoft изпраща поправки на повече от 100 недостатъка в своите продукти и четвърти пореден месец, в който поправките са над 120.

Сред основните заплахи за организациите този месец е CVE-2020-16875, която включва критичен недостатък в имейл софтуера Microsoft Exchange Server 2016 и 2019. Нападателят може да използва грешката на Exchange, за да стартира код по свой избор, само като изпрати booby- блокиран имейл до уязвим сървър на Exchange.

За компаниите е неприятна и CVE-2020-1210, недостатък на дистанционното изпълнение на код в поддържаните версии на софтуера за управление на документи на Microsoft Sharepoint, който нападатели могат да атакуват, като качат файл на уязвим сайт на Sharepoint. Microsoft отстрани поне пет други сериозни грешки във версиите на Sharepoint от 2010 до 2019 г., които също могат да бъдат използвани за компрометиране на системи, работещи с този софтуер.

Patch Tuesday не се отнася само до актуализациите на Windows: Google изпрати критична актуализация за своя браузър Chrome, която отстранява поне пет недостатъка в сигурността, които са оценени с висока степен на сериозност. Ако използвате Chrome и забележите икона с малка стрелка нагоре в кръг вдясно от адресната лента, е време да актуализирате. Затварянето на Chrome и рестартирането му трябва да приложи чакащите актуализации.

За пореден път няма налични актуализации на защитата за Flash Player на Adobe, въпреки че компанията достави софтуерна актуализация, която не е защитена за приставката на браузъра. Последният път, когато Flash получи актуализация на защитата, беше юни 2020 г., което може да предполага, че изследователите и / или нападателите са спрели да търсят недостатъци в нея. Adobe казва, че ще оттегли приставката в края на тази година, а Microsoft заяви, че планира напълно да премахне програмата от всички браузъри на Microsoft чрез Windows Update дотогава.

Преди да актуализирате с пакета за корекции за този месец, моля, уверете се, че сте архивирали вашата система и/или важни файлове. Не е необичайно актуализациите на Windows да пренасочват нечия система или да не позволяват да се стартира правилно, а за някои актуализации дори да се знае, че изтриват или повреждат файлове.

Така че направете си услуга и архивирайте, преди да инсталирате каквито и да е корекции. Windows 10 дори разполага с някои вградени инструменти, които ще ви помогнат да направите това, или за всеки файл / папка, или като направите едновременно пълно копие на вашия твърд диск.

И ако искате да сте сигурни, че Windows е настроен на пауза за актуализиране, за да можете да архивирате вашите файлове и / или система, преди операционната система да реши да рестартира и инсталира корекции по свой график, вижте това ръководство.

За повече информация:

https://krebsonsecurity.com/2020/09/microsoft-patch-tuesday-sept-2020-edition/

Palo Alto Networks закърпи 6 уязвимости в защитната стена

10 септември 2020 г.

Фирмата за сигурност Positive Technologies откри четири уязвимости в PAN-OS на Palo Alto Networks, софтуерът, който управлява защитните стени от следващо поколение на компанията. Разработчикът на защитните стени е издал корекции за тях, както и за няколко други.

Три недостатъка са оценени като много сериозни, един е оценен като среден, а други два са по-малко тежки.

Palo Alto Networks потвърди недостатъците и публикува корекции. Препоръчва на потребителите да ги приложат възможно най-скоро.

Нападателите могат да използват тези уязвимости, за да получат достъп до чувствителни данни или да развият атаката, за да получат достъп до вътрешни сегменти на мрежата на компания, която използва уязвими инструменти за защита.

Уязвимостите могат да бъдат използвани за получаване на максимални привилегии в операционната система, позволявайки на хакер да извърши каквото и да е действие с администраторски права, като например да стартира произволни системни команди или да предизвика отказ от услуга.

Трите уязвимости с висока степен на сериозност са:

CVE-2020-2036 е reflected cross-site scripting с тежест 8,8 по CVSS. За да се възползва от този недостатък, нападателят трябва да привлече администратор с активна удостоверена сесия в интерфейса за управление на защитната стена да щракне върху специално създадена връзка. Това може да позволи произволно изпълнение на JavaScript код в браузъра на администратора и да даде администраторски права на хакера. Атаката може да се извърши от интернет, но ако администраторският панел е разположен вътре, нападателите ще трябва да знаят адреса му в мрежата.

CVE-2020-2037 е уязвимост при инжектиране на команди с тежест 7.2 по CVSS. Тя може да позволи изпълнението на произволни команди на ОС в защитната стена. За да се възползва от този недостатък, нападателят трябва да получи разрешение в уеб интерфейса за управление на софтуерни данни. След това може да получи достъп до

специална секция на защитната стена, да постави злонамерен код в един от уеб формулярите и да получи максимални привилегии в операционната система.

CVE-2020-2038 е уязвимост при инжектиране на команди в операционната система и е с тежест 7.2 по CVSS. Уязвимостта беше открита в софтуерния интерфейс PAN-OS. Той разширява набора от системни команди, позволявайки различни потенциални атаки.

Недостатъкът, оценен със среден риск, е CVE-2020-2039 и може да позволи на неоторизиран потребител да качва произволни файлове с всякакъв размер в определена директория на сървъра на защитната стена, което може да доведе до атака от типа отказ от услуга . За да използват тази уязвимост, атакуващите могат да качат неограничен брой файлове с различни размери, което може напълно да изчерпи свободното пространство в системата, което прави администраторския панел недостъпен и уязвим за атаки.

Изследователите на Positive Technologies откриха и два други по-малко значими недостатъка в PAN-OS:

CVE-2020-2040 може да позволи на хакерите да нарушат системните процеси и потенциално да изпълнят произволен код с root права, като изпращат злонамерена заявка до captive портала или интерфейса за многофакторно удостоверяване. Тази уязвимост засяга всички версии на PAN-OS 8.0.

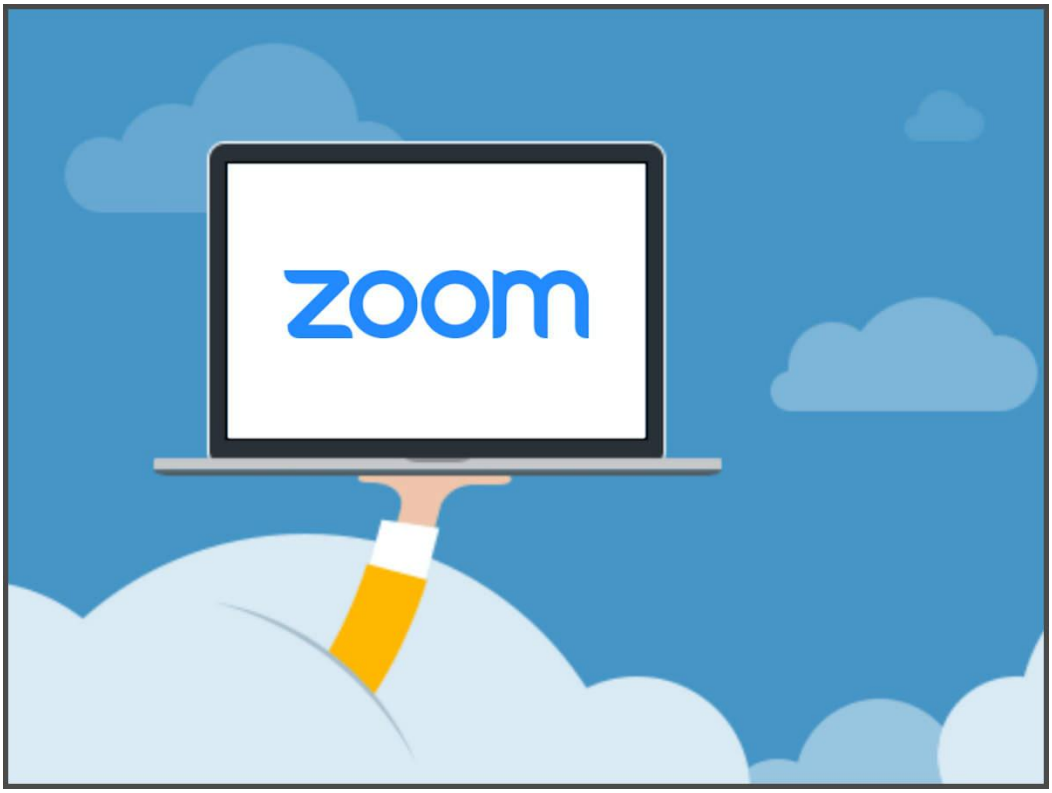
CVE-2020-2041 е несигурна конфигурация на приложението на Palo Alto Networks PAN-OS 8.1, която може да позволи на отдалечен неупълномощен потребител да изпрати заявка до устройство, причинявайки срив в услугата.

За повече информация:

https://www.bankinfosecurity.com/palo-alto-networks-patches-6-firewall-vulnerabilities-a-14977

Zoom прави двуфакторната автентикация (2FA) достъпна за всички свои потребители

15 септември 2020



Zoom вече поддържа телефонни обаждания, текстови съобщения и приложения за удостоверяване като форми на двуфакторно удостоверяване.

Zoom пуска поддръжка за двуфакторно удостоверяване (2FA) в своите уеб, настолни и мобилни приложения, което позволява на потребителите да удвоят сигурността на своите акаунти с допълнителен слой защита.

Системите 2FA изискват от потребителите да преминат предизвикателства за удостоверяване, които се нуждаят от отговори от два различни фактора. Има три класически фактора за удостоверяване, които често се използват - нещо, което знаете като парола или ПИН код, нещо, което имате - като физически ключове или приложения за удостоверяване, и нещо, което сте, това включва биометрични данни като пръстови отпечатъци или сканиране на ретината.

Платформата за видеоконференции обяви новата функция за сигурност, заявявайки: „Подобреното двуфакторно удостоверяване на Zoom (2FA) улеснява администраторите и организациите да защитават своите потребители и да предотвратяват нарушения в сигурността директно от нашата собствена платформа.“

Компанията потвърди, че предоставя функцията на всички свои потребители, включително тези, които използват нейния безплатен план.

Zoom описа и начините, по които потребителите могат да се удостоверяват, докато влизат в акаунтите си, „С ZoFA 2FA потребителите имат възможност да използват приложения за удостоверяване, които поддържат протокол за еднократна парола (TOTP), базиран на времето (като Google Authenticator, Microsoft Authenticator, и FreeOTP), или Zoom изпраща код чрез SMS или телефонно обаждане като втори фактор в процеса на удостоверяване на акаунта. "

Компанията за видео комуникация също така позволява на потребителите да използват кодове за възстановяване, за да влязат в акаунтите си, в случай че устройството им бъде изгубено или откраднато. Можете да проверите целия процес на активиране на 2FA, както и да използвате кодове за възстановяване в помощния център на платформата Zoom.

За повече информация:

https://www.welivesecurity.com/2020/09/15/zoom-2fa-available-users/