CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 18.05.2020 г.

Съдържание

Европейските суперкомпютри хакнати при мистериозни кибератаки

17 май 2020

Няколко високоефективни компютри (High-Performance Computers - HPC) и центрове за данни, използвани за изследователски проекти, бяха затворени в цяла Европа поради инциденти със сигурността.

Около дузина от тези суперкомпютри са засегнати в Германия, Великобритания и Швейцария, което не позволява на изследователите да продължат работата си. Някои от тях бяха компрометирани още през януари.

Суперкомпютрите са изключително мощни системи, изградени на базата на традиционен хардуер за извършване на високоскоростни изчисления. Те се използват главно за научна работа и тестване на математически модели за сложни физически явления и дизайни.

От Великобритания и Германия започнаха да съобщават за затварянето на суперкомпютрите след кибератаки.

ARCHER, националната служба за суперкомпютри в Обединеното кралство, стана недостъпна за изследователите на 11 май поради експлоатация в сигурността на своите входни възли. Услугата остава заключена за външен достъп. Задачите, които понастоящем се изпълняват или са на опашка, ще продължат да се изпълняват, но няма да е възможно влизането или задаването на нови задачи. Други източници информират, че всички съществуващи ARCHER пароли и SSH ключове ще бъдат нулирани. Потребителите, които влизат, когато услугата отново стане достъпна онлайн, ще се нуждаят от два вида идентификационни данни: SSH ключ с парола и нова ARCHER парола.

Проектът за високоефективни изчисления в Баден-Вюртемберг (bwHPC) в Германия в същия ден обяви инцидент със сигурността, който направи пет от неговите клъстери недостъпни, без да определи времеви рамки за възобновяване на операциите.

На 14 май суперкомпютърният център Лайбниц уведоми потребителите, че инцидент със сигурността е засегнал високоефективните му компютри, като накара института да ги изолира от външния свят.

Също на 14 май суперкомпютърният център Jülich в Германия обяви, че неговите суперкомпютри JURECA, JUDA и JUWELS стават недостъпни поради инцидент със ИТ сигурността.

До края на миналата седмица най-малко девет суперкомпютърни центъра в Германия са били засегнати от кибератаки.

Подобен проблем е публикуван и за системата Телец в Техническия университет в Дрезден: „Поради проблем със сигурността временно сме затворили достъпа до Телец.“

BwForCluster NEMO във Фрайбург, използван за изследвания в невронауката, физиката на елементарните частици и инженерството на микросистеми, също беше хакнат.

Beuth съобщава, че потребителите са получавали имейли, в които се казва, че начинът на нападателя да осъществи атаката е да открадне акаунт с root права. Открити са общо седем атаки, първата на 9 януари.

На 16 май Швейцарският център за научни изчисления (CSCS) информира своите потребители, че няколко високоефективни компютърни и академични центрове за данни вече не могат да бъдат достъпни поради злонамерена дейност, открита в системите.

Детайли за целта на атаката са оскъдни, но Европейската мрежова инфраструктура (EGI) публикува подробности за две от кибератаките, удрящи академични центрове за данни, които изглежда са дело на един и същи участник. И в двата случая нападателят използва компрометирани SSH идентификационни данни, за да преминава от един хост на друг и да злоупотребява с ресурси на процесора за добив на криптовалутата Monero. Някои хостове се използват за добив, други са прокси сървъри за свързване към минния сървър.

Екипът за реакция при инциденти в компютърната сигурност (CSIRT) в EGI установи, че в един от случаите злонамерената минна дейност е конфигурирана да работи само през нощта, най-вероятно за да се избегне откриването. Екипът разкри технически подробности и индикатори за анализираните от тях инциденти, отбелязвайки, че жертвите се намират в Китай, САЩ и Европа.

Изследователите твърдят, че един компонент на злонамерения софтуер има root права и зарежда други програми. Друг компонент се използва за премахване на следите от данните в дневника.

Изследователите твърдят също, че и двата компонента са двоични файлове ELF64. Зареждащото устройство е поставено под „/etc/fonts/.fonts“, а устройството за почистване на журнала е под „/etc/fonts/.low“.

За повече информация:

https://www.bleepingcomputer.com/news/security/european-supercomputers-hacked-in-mysterious-cyberattacks/

Обезпечаване на интелигентната инфраструктура по време на пандемията COVID-19

18 май 2020 г.

Обезпечаването на интелигентните домове и интелигентните сгради от рискове в киберсигурността става по-актуално от всякога по време на пандемичната криза COVID-19. ENISA представя някои основни мерки за осигуряване сигурността на интелигентните устройства.

Интернет на нещата

Интернет на нещата (IoT) промени начина, по който хората живеят, правят бизнес и си взаимодействат. Сградите и домовете стават все по-умни, по-сложни и по-свързани. Тази масивна взаимовръзка води до нова ефективност и възможности за потребителите, организациите и градовете. Независимо от това, тези предимства носят големи предизвикателства и рискове за киберсигурността.

Обезпечаването на интелигентните домове и интелигентните сгради от рискове в киберсигурността става по-актуално от всякога по време на пандемичната криза COVID-19. Хората прекарват значително време у дома, използвайки интелигентни

телекомуникации, за да поддържат връзка с бизнеса, лекарите, правителството, училището, приятелите и семейството си. Използвайки съвременните технологии, хората остават продуктивни за работата и домакинството си, но също така стават по-податливи на атаки от страна на участници в заплаха, които искат да спечелят пари.

ENISA за IoT и интелигентната инфраструктура

Агенцията работи върху сигурността на IoT от няколко години, разработвайки основни препоръки за сигурност на IoT. За повече информация: enisa.europa.eu/iot

Осигуряване сигурността на дома

Социалното дистанциране измести ежедневните навици с дейности, свързани с работа, образование, здравеопазване и социализация основно от дома. Повечето от тези дейности се извършват в цифров формат и затова те разчитат в голяма степен на свързаност и умни домашни устройства. Много потребители са наясно, че техните интелигентни устройства потенциално биха могли да въведат уязвимости в домашната им мрежа и трябва да ги конфигурират правилно. По-долу ENISA представя някои основни мерки за осигуряване сигурността на интелигентните устройства:

- Използвайте дълги пароли, двуфакторна или многофакторна автентификация и, ако има такива, активирайте биометрични функции или допълнителни ПИН кодове.
- Използвайте различни пароли за всяко устройство от вашата домашна мрежа.
- Спазвайте ръководствата за потребителя и активирайте съответните функции за защита при първоначална настройка.
- Активирайте известията за актуализация и извършвайте актуализации редовно
- Избягвайте въвеждането на чувствителна информация и бъдете наясно с начина, по който тя се използва.
- Изключете устройството, когато вече не се използва.
- Конфигурирайте няколко мрежи на вашия рутер и дръжте интелигентните си устройства в отделна Wi-Fi мрежа.
- Почистете интелигентното си устройство и използвайте функцията „фабрично нулиране“, преди да го изхвърлите или върнете.

Осигуряване на бизнес помещенията

Почти за една нощ, в опит за незабавно прилагане на социално дистанциране, много служители по целия свят започнаха да работят отдалечено от дома и далеч от офисите. Извън нормалната и обичайна за бизнеса ситуация, при прилагането на правилата за социално дистанциране и персонала, който работи на ротационен принцип, служителите трябва просто да бъдат малко по-усърдни по отношение на практиките за сигурност. Никога не е било по-важно проактивното обезопасяване на интелигентните сгради / офиси, които често контролират системи или операции като центрове за данни например.

Сигурността на мрежите, наблюдението на мрежовите аномалии, идентифицирането на злонамерено поведение, включително социално инженерство и опити за фишинг, както и прегледът на конфигурациите за сигурност на IoT е пътят напред и в това отношение ENISA предоставя следните препоръки в допълнение към посочените по-горе:

- Активирайте защитата на защитната стена и се уверете, че корпоративната мрежа е достъпна само за легитимни услуги.
- Деактивирайте неизползваните портове.
- Прилагайте мрежова микросегментация чрез създаване на виртуални мрежи, за да изолирате IoT системи от други критични ИТ системи.
- Активирайте мониторинга и диагностиката и ги следете редовно.
- Подгответе и актуализирайте плановете за реагиране при инциденти според текущите рискове.

Умните домове и интелигентните сгради са се превърнали в дигитални убежища за всички хора в социална изолация. Осигуряването им е споделена отговорност и всеки трябва да участва в постигането на по-сигурна и устойчива цифрова среда както у дома, така и на работното място.

За повече информация:

https://www.enisa.europa.eu/news/enisa-news/securing-smart-infrastructure-in-covid-19-pandemic