Эксплойт доступен каждому. Лишь обновление до последней версии спасёт веб-экосистему от RCE.

Исследователи безопасности из тайваньской компании DEVCORE обнаружили серьёзную уязвимость, затрагивающую установки PHP — это скриптовый язык программирования, широко используемый для разработки веб-приложений. Он может быть встроен в HTML-код и обычно работает на сервере, обрабатывая запросы от клиентов. PHP применяется для создания динамических веб-страниц, работы с базами данных, формирования и отправки электронной почты, управления сессиями и cookie, а также для многих других задач на веб-сервере." data-html="true" data-original-title="PHP" >PHP на Windows — это операционная система для персональных компьютеров, разработанная и выпускаемая компанией Microsoft. ОС предоставляет пользователю удобный интерфейс и обширный функционал для работы с компьютером. Первая версия Windows вышла в 1985 году.

 С помощью Windows пользователи могут закрывать целый спектр различных потребностей, будь то работа, учёба, развлечения, разработка программного обеспечения и т.п.

 Windows поддерживает широкий спектр аппаратного обеспечения, что делает её самой популярной и широко используемой настольной ОС в мире, способной, впрочем, работать также и на мобильных устройствах.
" data-html="true" data-original-title="Windows" >Windows в режиме CGI. Получившая идентификатор CVE-2024-4577 (рейтинг CVSS пока не определён), проблема позволяет злоумышленникам производить подстановку аргументов командной строки, что способно привести к удалённому выполнению кода (Remote Code Execution (RCE) — это критическая уязвимость, которая позволяет злоумышленнику дистанционно запустить вредоносный код в целевой системе по локальной сети или через Интернет. При этом физический доступ к устройству не требуется.

 В результате эксплуатации RCE-уязвимости киберпреступник может перехватить управление системой или ее отдельными компонентами, а также похитить конфиденциальные данные." data-html="true" data-original-title="RCE" >RCE).

Как сообщают специалисты DEVCORE, проблема «растёт» из другой уязвимости — CVE-2012-1823 , так как свежевыявленный баг позволяет обойти внедрённую от неё защиту с помощью определённых последовательностей символов.

CVE-2024-4577 затрагивает все версии PHP, установленные в операционной системе Windows, а именно:

Из-за повсеместного использования PHP в веб-экосистеме, а также простоты использования уязвимости, специалисты классифицировали её как критическую и

незамедлительно сообщили о ней официальной команде PHP. Отчёт об уязвимости был опубликован уже после выхода исправленной версии PHP, доступного для скачивания на официальном сайте.

По мнению экспертов, уязвимость потенциально может затронуть миллионы веб-сайтов и сервисов, работающих на Windows-серверах с PHP в режиме CGI. Тем не менее, на момент написания исследовательской статьи было подтверждено лишь то, что неавторизованный злоумышленник может напрямую выполнить произвольный код на удалённом сервере в следующих локализациях интерфейса: традиционный китайский, упрощенный китайский, японский.

Для экземпляров Windows, работающих в других локализациях, из-за широкого спектра сценариев использования PHP, как сообщают авторы исследования, в настоящее время невозможно полностью перечислить или исключить все возможные сценарии использования.

Администраторам рекомендуется провести самостоятельную комплексную оценку активов, проверить свои сценарии использования и обновить PHP до последней версии для обеспечения безопасности.

Стоит также учитывать, что эксплойт для данной уязвимости уже был разработан и опубликован специалистами из watchTowr Labs — это центр экспертизы по наступательной безопасности. В блоге центра публикуются результаты исследований, анализы уязвимостей, а также методики этичного хакинга, позволяющие различным компаниям укреплять свою кибербезопасность." data-html="true" data-original-title="watchTowr Labs" >watchTowr Labs, охарактеризовавшими его как легковоспроизводимый. В связи с этим, затягивать с переходом на исправленную версию PHP явно не стоит.

Кроме того, для предотвращения возможных атак рекомендуется также регулярно проверять конфигурации серверов, проводить аудиты безопасности и обучать сотрудников правилам безопасного использования и администрирования систем.

На перекрестке науки и фантазии — наш канал