Кибербандитам даже не нужно знать учётные данные, чтобы скомпрометировать вашу систему.

Компания Veeam призывает всех пользователей Veeam Backup Enterprise Manager обновить программное обеспечение до последней версии из-за обнаруженной критической уязвимости, позволяющей злоумышленникам обходить средства защиты аутентификации.

Veeam Backup Enterprise Manager — это централизованное решение для управления резервными копиями в инфраструктуре Veeam. Оно предоставляет единый веб-интерфейс для мониторинга, отчетности и управления заданиями резервного копирования, репликации и восстановления.

Платформа позволяет администратору легко управлять масштабными резервными копиями, выполнять поиск и восстановление отдельных файлов, а также управлять правами доступа пользователей и групп. Кроме того, Veeam Backup Enterprise Manager упрощает администрирование и повышает эффективность работы с данными в крупных IT-средах.

Уязвимость, получившая идентификатор CVE-2024-29849 и оценку 9.8 по шкале CVSS (Common Vulnerability Scoring System) — это открытый стандарт, используемый для оценки и классификации уязвимостей информационной безопасности. CVSS предоставляет числовую оценку, которая помогает организациям определить серьезность уязвимости и принять соответствующие меры для устранения угроз.

 Оценка CVSS представлена числовым значением от 0 до 10, где 0 обозначает отсутствие уязвимости, а 10 — наивысший уровень уязвимости. Эта оценка позволяет IT-специалистам и администраторам принимать решения о приоритетах по обеспечению безопасности систем и принимать меры для устранения уязвимостей, наиболее критичных для организации." data-html="true" data-original-title="CVSS" >CVSS, позволяет неавторизованному атакующему войти в веб-интерфейс Veeam Backup Enterprise Manager под именем любого пользователя.

Также компания сообщила о трёх других уязвимостях, влияющих на тот же продукт:

Все эти уязвимости были исправлены в версии 12.1.2.172. Важно отметить, что установка Veeam Backup Enterprise Manager не является обязательной, и те среды, в которых он не установлен, не подвержены данным уязвимостям.

За последние недели компания также устранила локальную уязвимость повышения

привилегий в Veeam Agent for Windows (CVE-2024-29853, оценка CVSS: 7.2) и критическую уязвимость удалённого выполнения кода в Veeam Service Provider Console (CVE-2024-29212, оценка CVSS: 9.9).

По словам Veeam, уязвимость CVE-2024-29212 связана с небезопасным методом десериализации, используемым сервером Veeam Service Provider Console (VSPC) при взаимодействии с агентом управления и его компонентами, что при определённых условиях позволяет выполнить удалённое выполнение кода на сервере VSPC.

Уязвимости в программном обеспечении Veeam Backup & Replication (CVE-2023-27532, оценка CVSS: 7.5) уже использовались такими группировками, как FIN7 и Cuba, для распространения вредоносных программ, включая вымогательские, что подчёркивает важность быстрой установки обновлений.