Cisco предупредила о критической уязвимости в программном обеспечении IOS XE для беспроводных контроллеров (WLC), получившей максимальный рейтинг опасности CVSS 10/10, сообщает BleepingComputer.

Уязвимость, обозначенная как CVE-2025-20188, позволяет злоумышленникам загружать произвольные файлы на устройство без авторизации, что может привести к удалённому выполнению кода (RCE) и полному захвату системы. Проблема связана с использованием фиксированного токена JWT (JSON Web Token), из-за чего атакующий может отправлять специально сформированные HTTPS-запросы к интерфейсу загрузки образов точек доступа.

Horizon3 опубликовала технические детали уязвимости, которые, хотя и не содержат готового эксплойта, дают достаточно информации для создания такового опытными хакерами. Cisco сообщила об уязвимости, выпустив патчи для версий IOS XE, начиная с 17.12.04. Уязвимость затрагивает устройства с включённой функцией Out-of-Band AP Image Download, которая позволяет загружать образы ОС через HTTPS.

Пользователям настоятельно рекомендуется обновить ПО, так как риск атак высок. Cisco подтвердила, что устройства с IOS (не XE), IOS XR, Meraki, NX-OS и AireOS не затронуты.