Критическая уязвимость в платформе Samsung MagicINFO 9 Server, обнаруженная в августе 2024 года, начала активно использоваться хакерами после публикации кода эксплойта. Об этом сообщили исследователи из Arctic Wolf.

Уязвимость, обозначенная как CVE-2024−7399, позволяет злоумышленникам без авторизации загружать вредоносные файлы на сервер, получая полный контроль над системой. Это особенно опасно, так как MagicINFO управляет экранами в магазинах, аэропортах и офисах.

Проблема связана с недостаточной проверкой загружаемых файлов: сервер не фильтрует имена и расширения, что позволяет хакерам размещать вредоносные JSP-файлы (JavaServer Pages) и выполнять произвольные команды. В результате устройства могут стать частью ботнета Mirai, используемого для кибератак. Эксплойт уже замечен в атаках.

Samsung устранила уязвимость в версии 21.1050, и компания настоятельно рекомендует обновить серверы. Arctic Wolf советует организациям ограничить доступ к серверам из интернета и усилить мониторинг. Уязвимость имеет рейтинг CVSS 8.8.