Портал Bleeping Computer сообщает, что более 16 000 сетевых устройств Fortinet были обнаружены взломанными с помощью нового бэкдора symlink, который позволяет получить доступ только для чтения к конфиденциальным файлам. Тем не менее речь идёт о масштабной и показательной кибератаке, причём уже на обновлённые для защиты устройства.

Некоммерческая организация The Shadowserver Foundation, собирающая и анализирующая данные о вредоносной активности в интернете, сообщила, что изначально было обнаружено 14 000 взломанных устройств. Компания Fortinet поспешила предупредить клиентов о новом механизме сохранения, используемом угрожающими субъектами (хакерами), для сохранения удалённого доступа к файлам в корневой файловой системе ранее взломанных, устройств серии FortiGate.

Представители Fortinet утверждают, что это не связано с эксплуатацией новых уязвимостей и относится к атакам, начавшимся в 2023 году. Хакеры использовали атаки нулевого дня для компрометации устройств на базе FortiOS. В новой атаке злоумышленники создавали символические ссылки и получали доступ на чтение к корневой файловой системе, даже после исправления уязвимостей. Символические ссылки соединяли пользовательскую файловую систему и корневую файловую систему в папке с языковыми файлами устройств. Поэтому хакеры и получали доступ.