Полномочия администратора дают хакерам безграничный доступ к скомпрометированным устройствам.

В нескольких моделях беспроводных роутеров D-Link обнаружена критическая уязвимость, позволяющая злоумышленникам без аутентификации получить административный доступ к устройствам. Уязвимость CVE-2024-6045 имеет высокий уровень опасности с оценкой 8.8 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.

По данным представителей TWCERT (Taiwan Computer Emergency Response Team) – тайваньская команда по реагированию на компьютерные инциденты. Она занимается мониторингом и анализом киберугроз, координирует действия по предотвращению и устранению инцидентов безопасности. TWCERT также предоставляет консультации и рекомендации по защите информационных систем, а также активно сотрудничает с международными организациями для повышения уровня кибербезопасности." data-html="true" data-original-title="TWCERT" >TWCERT, проблема вызвана нераскрытым встроенным тестовым бэкдором в конкретных моделях роутеров D-Link. Злоумышленники могут активировать Telnet-сервис, используя определённый URL, а также получить учётные данные администратора, анализируя прошивку роутера. Успешная атака даёт полный контроль над скомпрометированным устройством.

Перечень уязвимых моделей роутеров включает: E15, E30, G403, G415, G416, M15, M18, M30, M32, M60, R03, R04, R12, R15, R18, R32.

Компания D-Link выпустила обновления прошивки для устранения этой уязвимости. Пользователям данных моделей рекомендуется срочно обновить прошивку до последней версии для защиты от потенциальной эксплуатации уязвимости.

Актуальная безопасная версия прошивки для каждой затронутой модели указана ниже:

Пользователи должны немедленно применить эти обновления прошивки для защиты своих устройств от атак. Регулярная проверка и обновление прошивки роутеров является важной мерой для обеспечения безопасности сетевых устройств.