

CyStack cho biết đã phát hiện lỗ hổng bảo mật nguy hiểm như hổng tít i nhĩ u tít b DNS-320 ShareCenter giúp kẻ xấu có thể truy cập vào toàn bộ dữ liệu của người dùng.



Thiết bị DNS-320 ShareCenter tồn tại lỗ hổng bảo mật nguy hiểm tại dữ liệu người dùng.

Thông tin từ Công ty CyStack cho hay, đơn vị này đã phát hiện một [lỗ hổng bảo mật](#) nguy hiểm như hổng tít i nhĩ u tít b DNS-320 ShareCenter. Đây là một giải pháp lưu trữ và chia sẻ dữ liệu phổ biến, thường dùng trong các doanh nghiệp và hộ gia đình do D-Link sản xuất. Lỗ hổng cho phép kẻ xấu có thể dễ dàng truy cập vào toàn bộ dữ liệu được lưu trữ trên thiết bị.

Ngay sau khi nhận được báo cáo của [CyStack](#), [D-Link](#) đã thông báo cho người dùng về việc cập nhật bản vá mới nhất cho sản phẩm DNS-320 để khắc phục lỗ hổng này

[tại đây](#)

Chuyên gia Nguyễn Hữu Trung, người tìm ra lỗ hổng cho biết: “DNS-320 là một thiết bị lưu trữ mạng phổ biến do mức giá rẻ và hỗ trợ nhiều tính năng chia sẻ tiện ích. Tuy nhiên, cũng chính vì thế mà nhiều tập tin riêng tư của người dùng có nguy cơ bị xâm hại. Tôi thì đi tìm nhóm nghiên cứu của CyStack phát hiện ra lỗ hổng này, có ít nhất 800 thiết bị đang chủ yếu như hổng.”

Lỗ hổng đã được gán mã CVE là CVE-2019-16057, một lỗi mã để danh các lỗ hổng bảo o

Một lỗ hổng phát hiện trong các sản phẩm công nghệ phổ biến trên thị trường, lỗ hổng cung cấp bởi MITRE (mã lỗi CVE và lỗ hổng bảo mật bởi Cơ quan An ninh nội địa Mỹ). Theo Viện tiêu chuẩn và kỹ thuật quốc gia Hoa Kỳ (NIST) thì lỗ hổng này được đánh giá là mức độ nghiêm trọng cao nhất (critical), với điểm số CVSS V2.0 là 10/10, CVSS V3.1 là 9.8/10.

“Nhóm nghiên cứu bảo mật tại CyStack tìm thấy lỗ hổng trong quá trình nghiên cứu và tính bảo mật của các thiết bị mạng của doanh nghiệp, bao gồm cả [DNS-320 ShareCenter](#) của D-link,” anh Trung chia sẻ. “Chúng tôi phát hiện ra điểm yếu của module đăng nhập của thiết bị, chức năng là tính năng SSL Login.”

“Chỉ mất vài phút thay đổi tham số, kỹ thuật công có thể đánh lừa hệ thống và đăng nhập thành công vào thiết bị với quyền cao nhất (root permission). Khi đó, toàn bộ dữ liệu lưu trữ trong thiết bị của người dùng, bao gồm phim, ảnh, nhạc, tài liệu,... đều có thể bị kẻ xấu truy cập,” đội điều tra CyStack cho biết.

Nguồn: Vietnam+