UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00161

WD MY BOOK STORAGE ATTACK WIPES DATA

DATE ISSUED: 28th June 2021

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

A Remote Code Execution (RCE) vulnerability is responsible for attackers being able to perform factory resets on the popular Western Digital My Book Network Attached Storage (NAS) devices erasing years of customer data.

BREAKDOWN

The devices are typically attached to computers via USB and an Ethernet cable to connect to the Local Area Network (LAN) enabling users to access files and make changes through Western Digital’s cloud platform. The mass data wipe leaves folders present but empties them of all contents and many users reported receiving factory reset messages. A user reported attempting to log back in and being presented with a landing page that had no option to reset passwords and would not accept their original password to access their device and files. These devices have been out of support since 2015 and this incident is currently under active investigation by Western Digital. In some cases drives were wiped even when they were behind firewalls and had cloud features disabled. “Western Digital WD My Book Live (all versions) has a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. It can be triggered by anyone who knows the IP address of the affected device.”

REMEDIATION STEPS

- Unplug all Western Digital My Book devices until further notice.

REFERENCES & RESOURCES

ARS Technica	https://arstechnica.com/gadgets/2021/06/mass-data-wipe-in-my-book-devices-prompts-warning-from-western-digital
Western Digital	https://community.wd.com/t/action-required-on-my-book-live-and-my-book-live-duo/268147
Threatpost	https://threatpost.com/my-book-live-wiped-rce-attacks/167270/