

Mass deletion of data from WD My Book Live devices may have involved more than one vulnerability

30 June 2021, by Bob Yirka



Credit: Pixabay/CC0 Public Domain

Security experts at Ars Technica and Censys have found a second vulnerability in Western Digital's My Book Live devices, suggesting the recent mass deletion of data from the devices may have involved more than one vulnerability. Western Digital has posted an [update](#) on the situation on its support page.

My Book Live devices are a type of external hard drive that was promoted by its maker as a personal cloud device. Users could back up their phone, tablet or [computer data](#) automatically, making use of their own personal cloud—eliminating the need for a third-party cloud provider. Unfortunately, that plan went south for My Book Live owners recently—overnight, someone hacked into their devices and deleted all their data.

Initial reports suggested that the hackers had carried off the attacks using a previously known [vulnerability](#) in the devices that was not fixed because WD had ceased selling and supporting them. That hack allowed a hacker to gain root

access through a firmware exploit. In addressing the mass loss of data, WD suggested that hackers had taken advantage of the known vulnerability. But now, researchers at Ars Technica and Censys have found a second vulnerability in My Book Live devices that could have also been used to carry out the attacks—and it was even simpler than the first one.

In the second, the attackers did not need full control over the device to delete the data; instead, it allowed them to execute a command remotely, without requiring a password. The exploit executed code on the [device](#) that deleted all of the files. That vulnerability was identified in 2011, a year after the drives were first introduced. The researchers also found code on the devices that could have been used to deactivate the deletion sequence, but it had been commented out by engineers at WD. WD claims a mix-up during refactoring led to the vulnerability. At this time, there are differing opinions regarding whether the massive data deletion was due to only one vulnerability or both. In any case, WD has offered to recover the data for impacted users.

More information:

www.westerndigital.com/support...ive-wd-mybookliveduo

© 2021 Science X Network

APA citation: Mass deletion of data from WD My Book Live devices may have involved more than one vulnerability (2021, June 30) retrieved 21 October 2021 from <https://techxplore.com/news/2021-06-mass-deletion-wd-devices-involved.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.