Western Digital Shuts Down Services Due to Cybersecurity Breach

Western Digital has shut down several of its services after detecting a security breach on its network, the digital storage giant announced on Monday.

The service outage, announced on April 2, impacts cloud, proxy, web, authentication, email, and push notification services, including My Cloud, My Cloud Home (Duo), My Cloud OS5, SanDisk Ibi, and SanDisk Ixpand Wireless Charger.

In a press release issued on April 3, the company said it's responding to an ongoing network security incident that involves an unauthorized third party gaining access to "a number" of its systems.

"Upon discovery of the incident, the Company implemented incident response efforts and initiated an investigation with the assistance of leading outside security and forensic experts. This investigation is in its early stages and Western Digital is coordinating with law enforcement authorities," WD said.

The company is working on restoring impacted services and infrastructure. At this point in the investigation, it confirmed that the hackers did manage to gain access to certain types of data stored on its systems. The nature and scope of the compromised data is being determined.

SecurityWeek has reached out to Western Digital to find out if the attack involved ransomware and whether any customer

information was compromised.

At the time of writing, WD does not appear to be mentioned on the leak site of any major ransomware group. However, even if the incident is a ransomware attack, if the intrusion is recent, the company will likely only be added to a leak website after negotiations have failed.

Related: Synology, QNAP, WD Warn Users About Vulnerabilities Exploited at Hacking Contest

Related: Zero-Day Vulnerability Exploited in Recent Attacks on WD Storage Devices

Related: Old Vulnerability Exploited to Hack, Wipe WD Storage Devices

Western Digital Shuts Down Services Due to Cybersecurity Breach