Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA ‘Must Patch’ List

The US Cybersecurity and Infrastructure Security Agency (CISA) has ordered federal agencies to patch three Veritas Backup Exec vulnerabilities exploited in ransomware attacks.

A data backup product, Veritas Backup Exec supports mixed environments, with support for desktop operating systems, virtual environments (such as VMware and Hyper-V), and cloud platforms (including Amazon S3, Microsoft Azure, and Google Cloud Storage).

Tracked as **CVE-2021-27876**, **CVE-2021-27877**, and **CVE-2021-27878**, the three issues that CISA has added to its ‘Must Patch’ list were disclosed in March 2021, when Veritas released patches.

All three issues were identified in the SHA Authentication scheme of the Veritas Backup Exec agent and could allow an attacker to access arbitrary files or execute arbitrary commands.

In September 2022, a Metasploit module exploiting these vulnerabilities was released, and the first in-the-wild exploitation attempts were observed one month later.

In a report last week, Mandiant warned that the three flaws have been exploited in Alphv (BlackCat) ransomware attacks, for initial access.

According to the cybersecurity firm, there are roughly 8,500

Veritas Backup Exec instances exposed to the internet, some of which might be vulnerable to these flaws.

Last month, Veritas updated its 2021 advisory to warn customers of the observed exploitation attempts: “a known exploit is available in the wild for the vulnerabilities below and could be used as part of a ransomware attack.”

In addition to the Veritas Backup Exec flaws, CISA also added to its Must Patch list CVE-2019-1388, a privilege escalation issue in Microsoft Windows Certificate Dialog, and CVE-2023-26083, an information disclosure bug in Arm Mali GPU kernel driver.

“There is evidence that this vulnerability may be under limited, targeted exploitation. Users are recommended to upgrade if they are impacted by this issue,” Arm noted on March 31.

CISA added the five security defects to its Known Exploited Vulnerabilities catalog on April 7. Per Binding Operational Directive (BOD) 22-01, federal agencies have until April 28 to apply the available patches where necessary.

Related: Zimbra Flaw Exploited by Russia Against NATO Countries Added to CISA ‘Must Patch’ List

Related: Google Links More iOS, Android Zero-Day Exploits to Spyware Vendors

Related: CISA Gets Proactive With New Pre-Ransomware Alerts

Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA ‘Must Patch’ List