VULNERABILITY BULLETINS

Zoho Releases Security Advisory for ManageEngine Desktop Central and Desktop Central MSP

TLP:WHITE

Dec 07, 2021

Zoho has released a security advisory to address an authentication bypass vulnerability (CVE-2021-40539) in ManageEngine Desktop Central and Desktop Central MSP. An attacker could exploit this vulnerability to take control of an affected system. According to Zoho, this vulnerability is being actively exploited in the wild.

The United States (US) Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the Zoho Vulnerability Notification and the Zoho ManageEngine Desktop Central and ManageEngine Desktop Central MSP security advisories and apply the recommended mitigations immediately.

The Health-ISAC Threat Operations Center (TOC) also recommends users and administrators to review previous US Coast Guard Cyber Command (CGCYBER), National Security Agency (NSA), CISA, and Federal Bureau of Investigation (FBI) joint alerts that have been published in this intelligence portal, including Joint Cybersecurity Advisory Confirms Continued APT Exploitation of CVE-2021-40539 in Zoho ManageEngine ADSelfService Plus and Update: Joint Advisory Report: APT Actors Exploiting Newly Identified CVE-2021-40539 in ManageEngine ADSelfService Plus.

Reference(s)	Health-ISAC, Health-ISAC, Manage Engine, Manage Engine, Manage Engine

CVE(s)
CVE-2021-40539

Release Date
Dec 07, 2021

Sources
Zoho Vulnerability Notification

Zoho ManageEngine Desktop Central

ManageEngine Desktop Central MSP

Alert ID 555af713

View Alert

Tags Zoho user authentication appliance, Zoho ManageEngine ADManager Plus, Zoho ManageEngine ADSelfService Plus, Zoho ManageEngine ServiceDesk Plus, Zoho

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.