UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00196

ZOHO PASSWORD MANAGER UNDER ATTACK

DATE ISSUED: 13th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A critical vulnerability in the ManageEngine ADSelfService Plus Platform allows authentication bypass or Remote Code Execution (RCE) is under active attack in the wild. Successful exploitation gives attackers access to the Zoho Password Manager and access to users Active Directory (AD) and cloud accounts.

BREAKDOWN

Zoho ManageEngine is a self-service password manager and single sign-on feature for AD and cloud apps meaning anyone who gains access may have unlimited access to AD, numerous other applications and any sensitive data associated with them. This zero-day attack affects the REST APO URLs in ADSelfService Plus using specially built requests, enabling subsequent attacks including RCE. A patch has been issued by Zoho for the vulnerability tracked as CVE-2021-40539 and affects all builds prior to 6114.

REMEDIATION STEPS

- Apply patches provided by Zoho immediately – upgrade to v6114.
- Ensure that ADSelfService Plus is not directly accessible from the internet.
- Check the logs in the \ManageEngine\ADSelfService Plugs\logs folder to check for indication of compromise. Search for /RestAPI/LogonCustomization and /RestAPI/Connection to indicate whether your installation is affected.
- Contact details for further information or assistance are provided in the Zoho resource below.

REFERENCES & RESOURCES

Zoho	https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html
	https://www.manageengine.com/products/self-service-password/service-pack.html
Threatpost	https://threatpost.com/zoho-password-manager-zero-day-attack/169303/