FORTINET

# OUTBREAK ALERTS

## Zoho ManageEngine Vulnerability

### An unauthenticated RCE in ManageEngine ServiceDesk Plus

https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44077-unauthenticated-rce-vulnerability-in-servicedesk-plus-msp-versions-10527-till-10529

CVEs: CVE-2021-44077

APT Actors are actively exploiting Zoho ManageEngine ServiceDesk Plus which is an IT help desk software with asset management. The exploit is tracked via CVE-2021-44077 and rated critical due to its capability for unauthenticated remote code execution (RCE).

**Background**

The ManageEngine ServiceDesk Plus released a security advisory on authentication bypass vulnerability.

**Announced**

Dec 2: CISA and FBI released an alert on active exploitation
https://us-cert.cisa.gov/ncas/current-activity/2021/12/02/cisa-and-fbi-release-alert-active-exploitation-cve-2021-44077-zoho
https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Dec 6: FortiGuard Labs published a threat signal report
https://www.fortiguard.com/threat-signal-report/4329/joint-cybersecurity-advisory-on-attacks-exploiting-zoho-manageengine-servicedesk-plus-vulnerability-cve-2021-44077

**Latest Developments**

On 2nd of December 2021, CISA has announced active exploitation of CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus. Based on FortiGuard statistics from the last few days, Malware using this vulnerability is active in the wild.

## PROTECT

**Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:**

- Reconnaissance
- Weaponization
- Delivery

#### AV

**Blocks exploitation of the Zoho ManageEngine Vulnerability**

| FortiGate | FortiWeb | FortiClient | FortiSASE | FortiMail | FortiCASB | FortiCWP |
|---|---|---|---|---|---|---|
| DB 89.07442 | DB 89.07442 | DB 89.07442 | DB 89.07442 | DB 89.07442 | DB 89.07442 | DB 89.07442 |

| FortiADC | FortiProxy |
|---|---|
| DB 89.07442 | DB 89.07442 |

#### AV (Pre-filter)

**Blocks exploitation of the Zoho ManageEngine Vulnerability**

| FortiEDR | FortiSandbox | FortiNDR |
|---|---|---|
| DB 89.07442 | DB 89.07442 | DB 89.07442 |

- Exploitation

#### IPS

**Blocks exploitation of the Zoho ManageEngine Vulnerability**

| FortiGate | FortiSASE | FortiNDR | FortiADC | FortiProxy |
|---|---|---|---|---|
| DB 19.219 | DB 19.219 | DB 19.219 | DB 19.219 | DB 19.219 |

- Installation
- C2
- Action

## DETECT

**Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:**

#### Outbreak Detection

| FortiAnalyzer |
|---|
| DB 1.00037 |

#### Threat Hunting

| FortiAnalyzer | FortiSIEM |
|---|---|
| v6.4+ | v6.4+ |

#### Content Update

| FortiSIEM |
|---|
| DB 314 |

## RESPOND

**Develop containment techniques to mitigate impacts of security events:**

#### Automated Response

**Services that can automatically respond to this outbreak.**

FortiXDR

#### Assisted Response Services

**Experts to assist you with analysis, containment and response activities.**

Incident Response

## RECOVER

**Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:**

#### NOC/SOC Training

**Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.**

NSE Training | Response Readiness

#### End-User Training

**Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.**

Security Awareness & Training

## IDENTIFY

**Identify processes and assets that need protection:**

#### Attack Surface Hardening

**Check Security Fabric devices to build actionable configuration recommendations and key indicators.**

Security Rating

## Additional Resources

| | |
|---|---|
| **CISA** | https://www.cisa.gov/uscert/ncas/alerts/aa21-336a |
| **Hacker News** | https://thehackernews.com/2021/12/cisa-warns-of-actively-exploited.html |
| **NIST** | https://nvd.nist.gov/vuln/detail/CVE-2021-44077 |
| **Packet Storm** | https://packetstormsecurity.com/files/165400/ManageEngine-ServiceDesk-Plus-Remote-Code-Execution.html |

Learn more about FortiGuard Outbreak Alerts