F#RTINET.

OUTBREAK ALERTS



An unauthenticated RCE in ManageEngine ServiceDesk Plus

Zoho ManageEngine Vulnerability

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

CVEs: CVE-2021-44077

Background

tracked via CVE-2021-44077 and rated critical due to its capability for unauthenticated remote code execution (RCE).

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

Dec 6: FortiGuard Labs published a threat signal report

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.

FortiMail

DB 89.07442

FortiCASB

DB 89.07442

FortiCWP

DB 89.07442

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

events:

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

FortiSASE

DB 89.07442

Weaponization

Delivery

Blocks exploitation of the Zoho ManageEngine Vulnerability

FortiClient

DB 89.07442

FortiNDR



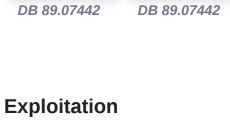








DB 89.07442 DB 89.07442





DB 19.219 DB 19.219 DB 19.219 DB 19.219



alert and generate reports:

Find and correlate important information to identify an outbreak, the following updates are available to raise



FortiAnalyzer

FortiSIEM



v6.4+

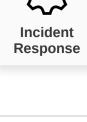
Automated Response Services that can automatically respond to this outbreak.

RESPOND

FortiXDR

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

Develop containment techniques to mitigate impacts of security events:



RECOVER

(and recovery from) security incidents:

Response

Readiness

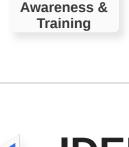
NOC/SOC Training

End-User Training

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

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

Improve security posture and processes by implementing security awareness and training, in preparation for



Security

Attack Surface Hardening Check Security Fabric devices to build actionable configuration recommendations and key indicators.

https://thehackernews.com/2021/12/cisa-warns-of-actively-exploited.html

Packet Storm https://packetstormsecurity.com/files/165400/ManageEngine-ServiceDesk-Plus-Remote-Code-Execution.html

NIST

CISA

Hacker News

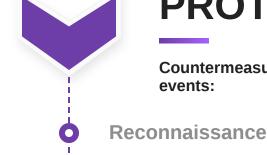






PROTECT







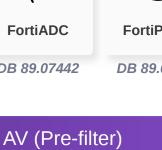


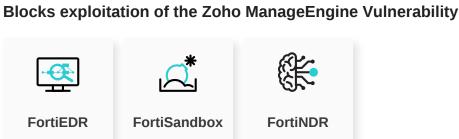


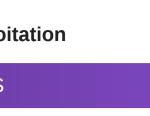




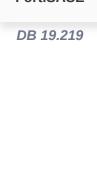




















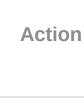




IPS Blocks exploitation of the Zoho ManageEngine Vulnerability













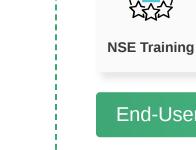








cyberattacks.









Additional Resources https://www.cisa.gov/uscert/ncas/alerts/aa21-336a

https://nvd.nist.gov/vuln/detail/CVE-2021-44077

Learn more about FortiGuard Outbreak Alerts