



Kaseya VSA Attack

Exploited by REvil Ransomware

<https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689>
 CVEs: [CVE-2021-30116](#), [CVE-2021-30119](#), [CVE-2021-30120](#)

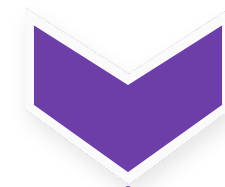
This report focusses on the Kaseya vulnerability itself -- A separate (dedicated) report is available for the REvil ransomware which exploits this vulnerability. Kaseya VSA product is the victim of a sophisticated cyberattack causing many of its customers to be infected with ransomware. On July 2, the SaaS version was temporarily shutdown, and Kaseya warned all its customers to immediately stop using the on-premise version until a patch is available. Nearly 40 of its MSP customers were reported hacked, who themselves manage hundreds or thousands of businesses underneath. <https://www.nbcnews.com/tech/security/ransomware-attack-software-manager-hits-200-companies-rcna1338> Background

Background The US-CERT is published at:
<https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-mssp-and-their-customers-affected-kaseya-vsa>

Announced The US-CERT is published at:
<https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-mssp-and-their-customers-affected-kaseya-vsa>

Latest Developments Kaseya has released patches for their VSA server. Kaseya has released a Compromise Detection Tool, which can be downloaded at the following link:
<https://kaseya.app.box.com/s/p9b712dcwfsnhuq2jmx31ibsuef6xict>
 More incident details have been provided at:
<https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961>
 VSA On premise runbook is provided at -
<https://helpdesk.kaseya.com/hc/en-gb/articles/4403709150993>
 VSA SaaS runbook is provided at -
<https://helpdesk.kaseya.com/hc/en-gb/articles/4403709476369>

July 11: Kaseya released final patch for VSA on-premise deployments, and started upgrading SaaS instances




PROTECT

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

- Reconnaissance
- Weaponization
- Delivery

Vulnerability

Detects vulnerable instance of Kaseya VSA running on Windows Server




FortiClient
DB 1.252


- Exploitation

IPS


IPS prevents the vulnerability on VSA on-premise instance from being exploited




FortiGate
DB 18.112



FortiSASE
DB 18.112



FortiNDR
DB 18.112



FortiProxy
DB 18.112


- 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 1.00033

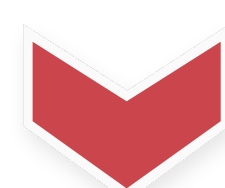
Threat Hunting



FortiAnalyzer
v6.2+



FortiSIEM
v6.2+




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 targeted 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

- Dark Reading** <https://www.darkreading.com/vulnerabilities-threats/attacks-on-kaseya-servers-led-to-ransomware-in-less-than-2-hours>
- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/kaseya-patches-vsa-vulnerabilities-used-in-revil-ransomware-attack/>
- Threat Singal** <https://www.fortiguard.com/threat-signal-report/4010>
- MSSP Alert** <https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/>

Learn more about [FortiGuard Outbreak Alerts](#)