Kaseya VSA Attack

Exploited by REvil Ransomware

https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689

CVEs: CVE-2021-30116

This report focusses on the Kaseya vulnerability itself -- A separate (dedicated) report is available for the REvil ransomware which exploits this vunlerability. 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

The US-CERT is published at:

https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

Announced

Kaseya publishes a detailed timeline of the incident at:

https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689

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 prmise 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

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*18.112*	IPS prevents the vulnerability on VSA on-premise instance from being exploited
FortiClient	**Vulnerability**	*1.252*	Detects vulnerable instance of Kaseya VSA running on Windows Server
FortiAnalyzer	**Event Handlers & Reports**	*6.2+*	Detects indicators attributed to Kaseya VSA vulnerability from Fabric products.
FortiSIEM	**Rules & Reports**	*6.2+*	Detects indicators attributed to Kaseya VSA vulnerability from Fabric products and 3rd party products.

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient
Vulnerability
Version Info: 1.252
Link: https://www.fortiguard.com/encyclopedia/endpoint-vuln/2262

Exploitation

FortiGate
IPS
Version Info: 18.112
Link: https://www.fortiguard.com/encyclopedia/ips/50557

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
Event Handlers & Reports
Version Info: 6.2+
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD52644

FortiSIEM
Rules & Reports
Version Info: 6.2+
Link: https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD52645