MUST READ: Ransomware: This new free tool lets you test if your cybersecurity is strong enough to stop an attack

Kaseya urges customers to immediately shut down VSA servers after ransomware attack

Victims are already seeing ransom demands ranging from $45,000 to $5 million.

By Jonathan Greig | July 2, 2021 -- 22:33 GMT (15:33 PDT) | Topic: Security

UPDATE: In a statement late Friday evening, Kaseya CEO Fred Voccola confirmed that the company's Incident Response team caught wind of the attack mid-day and immediately shut down their SaaS servers as a precautionary measure, despite not having received any reports of compromise from any SaaS or hosted customers.

"[We] immediately notified our on-premises customers via email, in-product notices, and phone to shut down their VSA servers to prevent them from being compromised. We then followed our established incident response process to determine the scope of the incident and the extent that our customers were affected," Voccola said.

"We engaged our internal incident response team and leading industry experts in forensic investigations to help us determine the root cause of the issue. We notified law enforcement and government cybersecurity agencies, including the FBI and CISA. While our early indicators suggested that only a very small number of on-premises customers were affected, we took a conservative approach in shutting down the SaaS servers to ensure we protected our more than 36,000 customers to the best of our ability."

So far, the company said they believe their SaaS customers "were never at-risk" and e[...] service to them in the next 24 hours once it is confirmed to be safe.

According to Voccola, about 40 customers worldwide were affected and the company is preparing a patch to mitigate the vulnerability for any on-premises victims.

"We've heard from the vast majority of our customers that they experienced no issues at all, and I am grateful to our internal teams, outside experts, and industry partners who worked alongside of us to quickly bring this to a successful outcome," Voccola added.

Comment sections on Reddit (https://twitter.com/GossiTheDog/status/1411140009709670406) are now inundated with responses from customers trying to respond to the attack and restore systems.

PREVIOUSLY: Kaseya has announced (https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021) that it is dealing with a massive ransomware attack that now may be affecting at least eight MSPs and hundreds of organizations.

In a message posted to its website, the remote management solutions provider said it is "experiencing a potential attack against the VSA that has been limited to a small number of on-premise customers only as of 2:00 PM EDT today."

"We are in the process of investigating the root cause of the incident with an abundance of caution but we recommend that you IMMEDIATELY shutdown your VSA server until you receive further notice from us," the company said.

"It's critical that you do this immediately, because one of the first things the attacker does is shut off administrative access to the VSA."

Kaseya has taken down all SaaS instances of its VSA remote monitoring and management tool in light of the attack.

John Hammond, senior security researcher at Huntress, told *ZDNet* that they were first notified of the attack at 12:35 ET and said it "has been an all-hands-on-deck evolution to respond and make the community aware."

Hammond attributed the attack to the prolific REvil/Sodinikibi ransomware group and Bleeping Computer (https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-200-companies-in-msp-supply-chain-attack/), The Record (https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/) and NBC News (https://www.nbcnews.com/tech/security/ransomware-attack-software-manager-hits-200-companies-rcna1338) all also reported that REvil or an affiliate was the culprit. Through an update to VSA software, REvil is allegedly spreading the ransomware widely.

"We cannot emphasize enough that we do not know how this is infiltrated in Kaseya's VSA. At the moment, no one does. We are aware of four MSPs where all of the clients are affected -- 3 in the US and one abroad. MSPs with over thousands of endpoints are being hit," Hammond said before Huntress updated its total to 8.

"We have seen that when an MSP is compromised, we've seen proof that it has spread through the VSA into all the MSP's customers. Kaseya's VSA could be either on prem or cloud hosted. They currently have all of their cloud servers offline for emergency maintenance."

Hammond added that three of Huntress' partners have been impacted, with "roughly 200 businesses encrypted."

He explained that agent.crt is dropped by the Kaseya VSA and is then decoded with certutil to carve out agent.exe, and inside agent.exe it has embedded `MsMpEng.exe` and `mpsvc.dll`.

```
/* WARNING: Globals starting with '_' overlap smaller symbols at the same address */

undefined4 __fastcall
WinMain(undefined param_1,undefined param_2,undefined param_3,undefined param_4,LPWSTR param_5)

{
  HRSRC pHVar1;
  HGLOBAL pvVar2;
  LPWSTR lpApplicationName;

  pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x65,L"SOFTIS");
  if (pHVar1 != (HRSRC)0x0) {
    pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
    if (pvVar2 != (HGLOBAL)0x0) {
      DAT_004143a0 = LockResource(pvVar2);
      pHVar1 = FindResourceW((HMODULE)0x0,(LPCWSTR)0x66,L"MODLIS");
      if (pHVar1 != (HRSRC)0x0) {
        pvVar2 = LoadResource((HMODULE)0x0,pHVar1);
        if (pvVar2 != (HGLOBAL)0x0) {
          _DAT_004143a4 = LockResource(pvVar2);
          FUN_00401000((int)_DAT_004143a4,0xc5588,L"mpsvc.dll");
          lpApplicationName = FUN_00401000((int)DAT_004143a0,0x56d0,L"MsMpEng.exe");
          _DAT_004143a8 = 0x44;
          CreateProcessW(lpApplicationName,param_5,(LPSECURITY_ATTRIBUTES)0x0,
                         (LPSECURITY_ATTRIBUTES)0x0,0,0x230,(LPVOID)0x0,(LPCWSTR)0x0,
                         (LPSTARTUPINFOW)&DAT_004143a8,(LPPROCESS_INFORMATION)&DAT_004143ec);
        }
      }
    }
  }
  return 0;
}
```

Manage Cookies

Huntress

"The legitimate Windows Defender executable was used to side-load a malicious DLL. It is the same exact binary for all victims," he said.

Huntress has a Reddit threat of updates (https://old.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/h3u5j2e/) about the situation and said there are indications that VSA admin user accounts are disabled only moments before ransomware is deployed.

CISA released a statement on Twitter (https://twitter.com/USCERT_gov/status/1411069203952640005) that said the organization is "taking action to understand and address the supply-chain ransomware attack against Kaseya VSA and the multiple MSPs that employ VSA software."

Mark Loman, a malware analyst for Sophos, shared a lengthy thread on Twitter about the attack and said some victims are already seeing a ransom page demanding $44,999 (https://twitter.com/markloman/status/1411053456983564300). Hammond told ZDNet that Huntress has seen ransom demands of $5 million already.

This is far from the first time Kaseya's tools have been used to spread a ransomware attack. As ZDNet has previously reported, REvil's predecessor Gandcrab leveraged Kaseya twice in 2019 to launch attacks, first using a Kaseya plugin (https://www.zdnet.com/article/gandcrab-ransomware-gang-infects-customers-of-remote-it-support-firms/) then VSA products (https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/) later that year.

Ransomware actors typically launch attacks on weekends or at night because there are less people watching systems.

Sophos released a detailed guide (https://community.sophos.com/b/security-blog/posts/active-ransomware-attack-on-kaseya-customers) for potential victims to figure out if they are under attack.

Chris Grove, technology evangelist with Nozomi Networks, said these types of supply chain attacks, like SolarWinds (https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/), go "straight to the jugular of organizations looking to recover from a breach."

"These types of technology management solutions can have high concentrations of risk due to their large collection of enterprise accounts with elevated privileges, unrestricted firewall rules needed for them to operate, and a cultural 'trust' that the traffic to/from them is legitimate and should be allowed," Grove said.

SOLARWINDS UPDATES

SolarWinds: The more we learn, the worse it looks (https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/)

CISA: US govt agencies must update right away (https://www.zdnet.com/article/cisa-updates-solarwinds-guidance-tells-us-govt-agencies-to-update-right-away/)

A second hacking group targets SolarWinds systems (https://www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/)

Hackers accessed Microsoft source code (https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/)

Microsoft quarantines trojanized apps (https://www.zdnet.com/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/)

Microsoft identifies 40+ victims, most in US (https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-solarwinds-hack/)

Microsoft and industry partners seize key domain used in hack (https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/)

SEC filing: 18,000 customers impacted (https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/)

Breach is not a marketing opportunity (https://www.zdnet.com/article/the-solarwinds-and-us-government-breach-is-not-a-marketing-opportunity/)

RELATED TOPICS: IT PRIORITIES | SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Jonathan Greig | July 2, 2021 -- 22:33 GMT (15:33 PDT) | Topic: Security