The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/12/2021

SUBJECT:
Multiple Vulnerabilities in Kaseya VSA Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Kaseya VSA that could allow for arbitrary code execution. Kaseya VSA is a software used by MSPs to remotely manage networks and endpoints. Successful exploitation of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
It is reported that at least 50 direct Kaseya customers were impacted leading to between 800 to 1500 downstream businesses being exploited with these vulnerabilities.

SYSTEMS AFFECTED:

- Kaseya VSA On-premises versions prior to 9.5.7a (9.5.7.2994)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Kaseya VSA that could allow for arbitrary code execution. These vulnerabilities can be exploited remotely if an attacker locates a vulnerable Kaseya Web interface. An attacker can exploit this issue to execute arbitrary code in the context of the running Kaseya server process. Details of these vulnerabilities are as follows:

Credentials leak and business logic flaw - CVE-2021-30116
XSS vulnerability - CVE-2021-30119

2FA bypass - CVE-2021-30120

Network IOCs

35.226.94[.]113
161.35.239[.]148
162.253.124[.]162

Endpoint IOCs

Filename	MD5 Hash	Function
cert.exe	N/A - File with random string appended	Legit certutil.exe Utility
agent.crt	939aae3cc456de8964cb182c75a5f8cc	Encoded malicious content
agent.exe	561cffbaba71a6e8cc1cdceda990ead4	Decoded contents of agent.crt
mpsvc.dll	a47cf00aedf769d60d58bfe00c0b5421	Ransomware Payload

Web Log Indicators

```
POST /dl.asp curl/7.69.1
GET /done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
GET /done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
POST /userFilterTableRpt.asp curl/7.69.1
```

Successful exploitation of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates and recommendations provided by Kaseya to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Kaseya:
https://www.kaseya.com/potential-attack-on-kaseya-vsa/
https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041
https://helpdesk.kaseya.com/hc/en-gb/articles/4403760102417

ZDNet:
https://www.zdnet.com/article/kaseya-ransomware-updates-attack-your-questions-answered/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30120