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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
04/20/2021
05/03/2021 – ***UPDATED***

SUBJECT:
Multiple Vulnerabilities in Pulse Connect Secure VPN Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Pulse Connect Secure VPN that could allow for remote code execution. Pulse Connect Secure VPN provides TLS and mobile VPN solutions. Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:
These vulnerabilities are currently being exploited in the wild by suspected state-sponsored threat actors to execute arbitrary code remotely on Pulse Connect Secure gateways.

SYSTEMS AFFECTED:
- Pulse Connect Secure prior to 9.1R.11.4

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 Pulse Connect Secure VPN that could allow for remote code execution. These vulnerabilities allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway, due to an authentication by-pass. Specifically this issue affects Pulse Connect Secure gateway. Exploitation of these vulnerabilities could facilitate remote code execution, privilege escalation, and lateral access to enterprise, operational technology, and cloud networks.

Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

May 3 – UPDATED TECHNICAL SUMMARY:

Details of the vulnerabilities are as follows:

- ***Multiple use after free in Pulse Connect Secure before 9.1R11.4 allows a remote unauthenticated attacker to execute arbitrary code via license server web services (CVE-2021-22893)***
- ***Buffer overflow in Pulse Connect Secure Collaboration Suite before 9.1R11.4 allows a remote authenticated users to execute arbitrary code as the root user via maliciously crafted meeting room (CVE-2021-22894)***
- ***Command Injection in Pulse Connect Secure before 9.1R11.4 allows a remote authenticated users to perform remote code execution via Windows File Resource Profiles (CVE-2021-22899)***
- ***Multiple unrestricted uploads in Pulse Connect Secure before 9.1R11.4 allow an authenticated administrator to perform a file write via a maliciously crafted archive upload in the administrator web interface (CVE-2021-22900)***

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade the Pulse Connect Secure server software version to the 9.1R.11.4
- Disabling Windows File Share Browser and Pulse Secure Collaboration features
- Block external access at the network boundary, unless external parties require service.
- If global access isn't needed, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of successful exploits.
- Run all software as a nonprivileged user with minimal access rights. To mitigate the impact of a successful exploit, run the affected application as a user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Deploy NIDS to detect and block attacks and anomalous activity such as requests containing suspicious URI sequences. Since the webserver may log such requests, review its logs regularly.
- Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploit attempts of memory-corruption vulnerabilities.

May 3 – UPDATED RECOMMENDATIONS:

- ***Apply the latest patch released by Pulse Secure***
- ***Run the Pulse Secure Connect Integrity Tool to help identify any malicious activity***

REFERENCES:
Bleeping Computer:
https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22893

Pulse Security:
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784

May 3 – UPDATED REFERENCES:
Pulse Security:
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/SA44784/ (PATCH)
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755 (Pulse Secure Connect Integrity Tool)

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.