*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**
**www.cisa.gov/tlp**
**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**
06/20/2022

**SUBJECT:**
A Vulnerability in Splunk Enterprise Deployment Servers Could Allow for Arbitrary Code Execution

**OVERVIEW:**
A vulnerability in Splunk Enterprise Deployment Servers Could Allow for Arbitrary Code Execution. Splunk Universal Forwarders, in which the vulnerability lies, are used to send data from a machine to a data receiver usually Splunk. If an attacker is able to compromise a Splunk

**THREAT INTELLIGENCE:**
There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- Splunk Enterprise deployment servers in versions prior to 9.0

**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:**

A vulnerability in Splunk Enterprise Deployment Servers in versions before 9.0 let clients deploy forwarder bundles to other deployment clients through the deployment server. An attacker that compromised a Universal Forwarder endpoint could use the vulnerability to execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server. When a deployment server is used, it allows the creation of configuration bundles that can be automatically downloaded by Splunk Universal Forwarder (SUF) agents or other Splunk Enterprise instances such as heavy forwarders. These configuration bundles can, among plain text configuration files also contain binary packages, most commonly used for specific connectors. The administrator of a deployment server controls which SUF can download what – this can be done by IP addresses, DNS names or architecture. Since these bundles can contain binary files, once fetched by a SUF, the SUF will execute it. By default, most SUF agents will run as SYSTEM on Windows. (CVE-2022-32158)

**Tactic**: *Execution* **(**TA0002**):**

**Technique**: *Software Deployment Tools* **(**T1072**):**

Exploitation of this vulnerability could allow for an attacker to execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate updates provided by Splunk to vulnerable systems immediately after appropriate testing. (**M1051: Update Software, M1042: Disable or Remove Feature or Program**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated

administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048 : Application Isolation and Sandboxing**)
    - **Safeguard 4.1 : Establish and Maintain a Secure Configuration Process:** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

**Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent

**REFERENCES:**

**Splunk:**
https://www.splunk.com/en_us/product-security/announcements/svd-2022-0608.html

https://docs.splunk.com/Documentation/Forwarder/8.2.6/Forwarder/Abouttheuniversalforwarder

**CVE:**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-321582