FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

16 NOV 2021

FLASH Number

AC-000155-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

An APT Group Exploiting a 0-day in FatPipe WARP, MPVPN, and IPVPN Software

Summary

As of November 2021, FBI forensic analysis indicated exploitation of a 0-day vulnerability in the FatPipe MPVPN® device software[1] going back to at least May 2021. The vulnerability allowed APT actors to gain access to an unrestricted file upload function to drop a webshell for exploitation activity with root access, leading to elevated privileges and potential follow-on activity. Exploitation of this vulnerability then served as a jumping off point into other infrastructure for the APT actors. This vulnerability is not yet identified with a CVE number but can be located with the FatPipe Security Advisory number FPSA006. The vulnerability affects all FatPipe WARP®, MPVPN, and IPVPN® device software prior to the latest version releases 10.1.2r60p93 and 10.2.2r44p1.

[1] A patented router clustering device.

The compromise of affected systems running FatPipe MPVPN software involves exploiting a servlet at the URL path `/fpui/uploadConfigServlet` and dropping a webshell `/fpui/img/1.jsp` with root privileges.

Technical Details

The following was executed for initial exploitation:

- GET request to `/RELEASE-NOTES.txt`
- POST request to `/fpui/uploadConfigServlet?fileNumber=undefined`

Immediately after the POST request, the following activity was observed:

- Download `<attacker_ip>/sshd_config`
- Download `<attacker_ip>/authorized_keys`
- Backup the system's current `SSHd` configuration file, `sshd_config`, and the "root" user's SSH authorized keys file, `/root/.ssh/authorized_keys`
- Overwrite the legitimate `sshd_config` and root user's authorized_keys files with the actor's malicious versions
- Restart the `SSHd` service

During a varying length of time while the webshell was available, the actor(s) used the new SSH access to route malicious traffic through the device and target additional U.S. infrastructure.

In most cases, after the exploitation activity was complete, the following activity was observed as part of a "clean-up" process to hide the malicious actor's activity and to protect their exploit until a later date:

- Restore original `sshd_config` and `authorized_keys` files and delete the malicious copies
- Overwrite the `btmp`, `wtmp`, and `lastlog` entries to hide their session activity
- Restart the `SSHd` service
- Delete the webshell at `<tomcat-installation-path>/webapps/fpui/img/1.jsp`

Indicators

- `<tomcat-installation-path>/webapps/fpui/img/1.jsp`
- `/etc/ssh/sshd_config.bak`
- `/root/.ssh/authorized_keys.bak`

- Search Tomcat access logs, located at `/var/log/tomcat/localhost_access_log*`, for:
  - POST requests to the URL: `/fpui/uploadConfigServlet?fileNumber=undefined`
  - GET requests to the URL, with commands: `/fpui/img/1.jsp`
- Search SSH access/secure logs under `/var/log` for successful SSH connections via public key from unknown IP addresses: `Accepted publickey for root`
- Search `wtmp` and `lastlog` files for sessions from unknown IP addresses
- Search Tomcat error logs, located at `/var/log/tomcat/catalina*`, for the following caught exception:

```
ERROR com.fatpipe.centralmanager.servlet.UploadConfigServlet-
Exception occurred while uploading config. Exception is : null
```

NOTE: Detection of exploitation activity may be difficult, as cleanup scripts designed to remove traces of the actor(s) activity were discovered in most cases.

Yara Signatures

```
rule APT_Webshell_1_jsp {
    strings:
        $s1 = "Runtime.getRuntime().exec(request.getParameter("
        $s2 = "request.getParameter(\"pwd\")"
        $s3 = "while((a=in.read(b))!=-1){"
    condition:
        filesize < 25KB and 2 of them
}
```

Information Requested:

Please report to FBI the existence of any of the following:

- Identification of indicators of compromise as outlined above.
- Presence of webshell code on compromised FatPipe WARP, MPVPN, and IPVPN appliances.
- Unauthorized access to or use of accounts.

- Evidence of lateral movement by malicious actors with access to compromised systems.
- Malicious IPs identified through the conducted log file searches and session activity.
- Suspicious or malicious .bash_history contents.
- Other indicators of unauthorized access or compromise.

Recipients of this information are encouraged to contribute any additional information that they may have related to this threat.

Recommended Mitigations:

Organizations that identify any activity related to these indicators of compromise within their networks should take action immediately.

FatPipe released a patch and security advisory, FPSA006, on November 16, 2021, that fixes the vulnerability. All FatPipe WARP, MPVPN, and IPVPN device software prior to releases 10.1.2r60p93 and 10.2.2r44p1 are vulnerable. The security advisory and additional details are available at the following URL: https://fatpipeinc.com/support/cve-list.php.

FBI strongly urges system administrators to upgrade their devices immediately and to follow other FatPipe security recommendations such as disabling UI and SSH access from the WAN interface (externally facing) when not actively using it.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication: the context and individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.