FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 Sep 2017

Alert Number

MC-000087-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@ic.fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, 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.*

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

This FLASH has been released **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Update to Apache Struts Vulnerabilities Compromise Corporate Web Servers

Summary

This is an update to the previously reported MC-000086-MW alert titled “Apache Struts Vulnerabilities Compromising Corporate Web Servers,” disseminated on 15 Sept 2017. This update includes the SHA256 hash values pertaining to the original Web shells (IOCs) originally provided.

Technical Details

Critical security vulnerabilities in the Apache Struts software enable cyber actors to compromise corporate Web servers, thereby putting sensitive corporate data at risk. The vulnerabilities allow for remote code execution (RCE) by sending a special request to a vulnerable server and dropping malware or other unauthorized code after access is gained. It potentially enables actors to locate and identify credentials, connect to the database server, and extract or delete the data. Organizations under attack may not immediately notice a compromise.

Apache Struts is an open source and widely used no-cost framework for Java application building. It is utilized across the financial services sector and other critical infrastructure. As such, these vulnerabilities affect numerous industries, including financial firms and third-party vendors on which financial firms rely. Vulnerabilities associated with Apache Struts can exist on Web applications hosted on traditional servers as well as be embedded in hardware devices such

as multifunction printers which support a Web interface for configuration and management.

During an incident involving one of the previously reported Apache Struts vulnerabilities, cyber actors deployed multiple Web shells. Below are the SHA256 hash values pertaining to the previously reported Web shells:

- SHA256: 0fe16dc5b71147d588b3a951a3d22d4d67cec32441adbf0e0f89c0706198def3
- SHA256: d370a3d3f571934f47a36a263e85a23a86dbaff433bcfb07e8c3f93424fecf3a
- SHA256: f4603dc44cb2f6fbcca8f3fcedaafff2ebd4db827e6b0cd8ee55519ea4252a94
- SHA256: de8c75a6cc93463254d72226ac546550f8449acd6c55223d263ae1f34f3dc141
- SHA256: 8fb2869e34396d3a26e33bfd54403f08bfea0d618fa8727590663c1e6deaf5a0
- SHA256: 09bf4661f8d5b8736be73ef1ba22a3ab6d08e8d6fd65a63eb7ea76e56ed6aa55
- SHA256: 6998873a969581460704631e42c0fa53da707b474dba97b872f715f6a9e86dbc
- SHA256: 684dc8d9908ff44e9bfc7bb045242600481ee2188de8cb2782135be9664c17de
- SHA256: d315530754c90fc05d91eb2cd4f50f67dcdf233bdd60ea2d591e4a292dd63bc6
- SHA256: 5bb73e9a41ee1e8ead70ed9fd3e9e7f0a253e84cb441b8c7889825364b62041e

Prevention and Mitigation

Web application vulnerabilities or configuration weaknesses are regularly exploited. Therefore, identification and closure of these vulnerabilities is crucial to avoiding potential compromise. The FBI suggests precautionary measures to mitigate the threats posed by these vulnerabilities, specifically patching and updating systems running Apache Struts. Patches to mitigate threats from Apache Struts vulnerabilities have been released and are currently publicly available. It is recommended to continue to monitor for new vulnerabilities and patches as they emerge. Also review reliance on easily identified Internet connected devices for critical operations, particularly those shared with public facing Web servers.

The following suggestions specify good security and Web server specific practices:

- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Implement a least-privileges policy on the Web server to:
    - Reduce adversaries' ability to escalate privileges or pivot laterally to other hosts.
    - Control creation and execution of files in particular directories.
- If not already present, consider deploying a demilitarized zone (DMZ) between your Web-facing systems and the corporate network. Limiting the interaction and logging traffic between the two provides a method to identify possible malicious activity.
- Ensure a secure configuration of Web servers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.
- Utilize a reverse proxy or alternative service, such as modsecurity, to restrict accessible URL paths to known legitimate ones.
- Establish, and backup offline, a "known good" version of the relevant server and a regular change-management policy to enable monitoring for changes to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero day attacks it will highlight possible areas of concern.

- Deploy a Web application firewall and conduct regular virus signature checks, application fuzzing, code reviews and server network analysis.

Detection

The following may be indicators that your Web server has been infected by malware. Note a number of these indicators are common to legitimate files. Any suspected malicious files should be considered in the context of other indicators and triaged to determine whether further inspection or validation is required.

- Abnormal periods of high site usage (due to potential uploading and downloading activity);
- Files with an unusual timestamp (e.g., more recent than the last update of the Web applications installed);
- Suspicious files in Internet-accessible locations (web root);
- Files containing references to suspicious keywords such as cmd.exe or eval;
- Unexpected connections in logs. For example:
    - A file type generating unexpected or anomalous network traffic (e.g., a JPG file making requests with POST parameters);
    - Suspicious logins originating from internal subnets to DMZ servers and vice versa.
- Any evidence of suspicious shell commands, such as directory traversal, by the Web server process.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@ic.fbi.gov or (202) 324-3691.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Administrative Note

This product is marked **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.