CIRMA
News & Alerts
CYBER SECURITY

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

July 30, 2025

Two CISA ToolShell Malware Analysis Reports - TLP: GREEN

CISA has provided the attached two **Malware Analysis Reports** related to the recent exploitation of Microsoft SharePoint vulnerabilities based on files received from third parties. The vulnerabilities include CVE-2025-53770 and CVE-2025-53771, which are variants or bypasses of previously disclosed flaws CVE-2025-49704 and CVE-2025-49706.

A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk (CISAservicedesk@cisa.dhs.gov).

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov. SLTT entities should also report to the MS-ISAC SOC.

These reports are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

> Click here for MAR-251132.r1.v2.GREEN.pdf

> Click here for MAR-251132.r2.v2.GREEN.pdf