CYBER ADVISORY

TLP:CLEAR

27 December 2024

Apache Multiple Vulnerabilities

Apache | MINA | HugeGraph | Traffic Control

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of three new Apache vulnerabilities, two rated critical, and one currently unrated. These vulnerabilities affect various Apache products.[1,2,3,4]

CVE-2024-52046, with a CVSS 4.0 score of 10, affects Apache MINA versions 2.1 – 2.1.9 and 2.2 – 2.2.3. This vulnerability allows attackers to exploit deserialization through specially crafted deserialization data, potentially leading to remote code execution (RCE) attacks.[5]

CVE-2024-43441, with no current CVSS rating, affects Apache HugeGraph-Server versions from 1.0.0 – before 1.5.0. This vulnerability allows for authentication bypass by Assumed-Immutable Data.[6]

CVE-2024-45387, with a current CVSS 3.1 score 9.9 and no current CVSS 4.0 score, affects Traffic Ops in Apache Traffic Control versions 8.0.0 – 8.0.1. This vulnerability allows a privileged user to execute structured query language (SQL) against the database by sending a specially-crafted (PUT) request.[7]

The Cal-CSIC recommends the following actions:

- Upgrade Apache MINA to versions 2.0.27, 2.1.10, and 2.2.4
  - In addition, Apache states users also need to explicitly allow the classes the decoder will accept in the ObjectSerializationDecoder instance, using one of the three methods listed here: CVE-2024-52046: Apache MINA: MINA applications using unbounded deserialization may allow RCE-Apache Mail Archives[8]
- Upgrade Apache HugeGraph-Server to version 1.5.0
- Upgrade Apache Traffic control to version 8.0.2

For further information on applying upgrades please refer to:

- CVE-2024-52046: Apache MINA: MINA applications using unbounded deserialization may allow RCE-Apache Mail Archives
- CVE-2024-43441: Apache HugeGraph-Server: Fixed JWT Token(Secret)-Apache Mail Archives
- CVE-2024-45387: Apache Traffic Control: SQL Injection in Traffic Ops endpoint PUT deliveryservice_request_comments-Apache Mail Archives

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Apache Warns of Critical Flaws in MINA, HugeGraph, Traffic Control;" https://www.bleepingcomputer.com/news/security/apache-warns-of-critical-flaws-in-mina-hugegraph-traffic-control/; accessed 26 December 2024
[2] NIST; "CVE-2024-52046 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-52046; accessed 26 December 24
[3] NIST; "CVE-2024-43441 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-43441; accessed 26 December 24

[4] NIST; "CVE-2024-45387 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-45387; accessed 26 December 24
[5] CVE Program; "CVE-2024-52046;" https://www.cve.org/CVERecord?id=CVE-2024-52046; accessed 26 December 24
[6] CVE Program; "CVE-2024-43441;" https://www.cve.org/CVERecord?id=CVE-2024-43441; accessed 26 December 24
[7] CVE Program; "CVE-2024-45387;" https://www.cve.org/CVERecord?id=CVE-2024-45387; accessed 26 December 24
[8] Apache; "CVE-2024-52046: Apache MINA: MINA applications using unbounded deserialization may allow RCE;" https://lists.apache.org/thread/4wxktgjpggdbto15d515wdctohb0qmv8; accessed 26 December 24