مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Nagios Log Server

Tracking #:432317788

Date:08-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that two severe vulnerabilities in Nagios Log Server that can be exploited by any authenticated user, including those with low privileges.

TECHNICAL DETAILS:

Security researchers have identified two severe vulnerabilities in Nagios Log Server that can be exploited by any authenticated user, including those with low privileges. CVE-2025-44823 enables attackers with valid API tokens to enumerate all users and retrieve plaintext administrative API keys, leading to potential full compromise of the log management system (CVSS 9.9). CVE-2025-44824 allows such users to force a shutdown of the internal Elasticsearch subsystem, causing a total loss of log ingestion, query, and alerting capability (CVSS 8.5). Working proof-of-concept exploits are available, making these flaws particularly high-risk for production deployments. Nagios released an update (2024R1.3.2) that fixes the issues.

Vulnerability Details:

1. **CVE-2025-44823**: API Key Disclosure & User Enumeration
   - **CVSS: 9.9 (Critical)** — Remote exploitation, full confidentiality and integrity loss, no user interaction required.
   - Description: Any authenticated API token (including low-privilege) can issue a get_users request, retrieving a full inventory of users and their plaintext API keys, including administrative credentials.
   - Risk: Enables privilege escalation and full system compromise via unauthorized use of leaked tokens.
   - PoC: Exploitation only requires a valid token. Simple API requests yield all user credentials; exploitation is trivial and exploits are public.

2. **CVE-2025-44824**: Elasticsearch Subsystem Shutdown
   - **CVSS: 8.5 (High)** — Availability impact, trivial exploitation
   - Description: Authenticated users (including low-privilege) can invoke API calls to stop the internal Elasticsearch service, disrupting all log ingestion, alerting, and historical searches.
   - Risk: Results in immediate loss of log visibility, impacting detection and compliance.

Affected version:

- Nagios Log Server before 2024R1.3.2

RECOMMENDATIONS:

- Apply Patches Immediately: Upgrade all Nagios Log Server instances to 2024R1.3.2 or newer as a matter of urgency, regardless of privilege or network exposure.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.nagios.com/changelog/#log-server