مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Kibana

Tracking #:432316236

Date:09-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Kibana, has issued a critical security advisory to address multiple critical vulnerabilities.

TECHNICAL DETAILS:

Kibana, the popular data visualization and analytics platform has released critical security advisory to address two critical vulnerabilities (**CVE-2024-37288 and CVE-2024-37285**) that pose significant risks to users. These vulnerabilities, which stem from YAML deserialization flaws, could allow attackers to execute arbitrary code on affected systems, potentially leading to complete system compromise.

1. **CVE-2024-37288**: CVSS Score: 9.9 (Critical)- Kibana arbitrary code execution via YAML deserialization in Amazon Bedrock Connector

- A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload.
- This issue only affects users that use Elastic Security's built-in AI tools 10 and have configured an Amazon Bedrock connector
- **Affected Version**: Kibana version 8.15.0.
- **Fixed Version**: Kibana version 8.15.1.

2. **CVE-2024-37285**- CVSS Score: 9.1 (Critical)-Widespread YAML Deserialization Vulnerability

- A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload.
- A successful attack requires a malicious user to have a combination of both specific Elasticsearch indices privileges and Kibana privileges assigned to them.
- **Affected Version**: Kibana versions 8.10.0 to 8.15.0
- **Fixed Version**: Kibana version 8.15.1.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected products to the fixed version at the earliest.

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://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119