VULNERABILITY BULLETINS

Urgent Kibana Patch for Severe Security Vulnerability, CVE-2024-37287

TLP:WHITE

Aug 07, 2024

On August 6, 2024, Elasticsearch released a security update regarding a critical vulnerability discovered in its popular open-source data visualization and exploration tool, Kibana.

The vulnerability, CVE-2024-37287, has a CVSS score of 9.9 and allows arbitrary code execution through a prototype pollution security flaw. This results in significant risks to self-managed and cloud-based instances of Kibana.

Specifically, the security flaw affects Kibana versions before 8.14.2 and Kibana 7.x versions before 7.17.23.

Health-ISAC is providing this information for situational awareness. Users are strongly advised to upgrade to Kibana versions 8.14.2 or 7.17.23 as soon as possible. These updates include patches that effectively mitigate the risk of arbitrary code execution.

The Elasticsearch team discovered a security flaw in Kibana that could allow adversaries to launch arbitrary code through a prototype pollution vulnerability. An attacker with access to machine learning and alerting connector features and write access to internal machine learning indices can trigger a prototype pollution vulnerability, ultimately leading to arbitrary code execution.

A prototype pollution vulnerability occurs when an adversary can modify the prototype of an object in JavaScript, allowing them to inject arbitrary properties that are then inherited by all instances of the affected object.

The vulnerability impacts various Kibana deployment instances, including self-managed installations, Docker images, Elastic Cloud, Elastic Cloud Enterprise (ECE), and Elastic Cloud on Kubernetes (ECK). Although certain environments limit code execution within containers, protection mechanisms associated with each affected instance can prevent additional exploitation, such as container escape.

Mitigations:

Organizations with affected Kibana instances should upgrade to version 8.14.2 and 7.17.23 to mitigate exposure to potential attacks and ensure the resiliency of their security apparatus.
Health-ISAC provides this information to prevent your security apparatus's successful exploitation and disruption. For more information, see Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.

Health-ISAC provides this information to prevent your security apparatus's successful exploitation and disruption. For more information, see Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.

Reference(s)	Security Online, Elastic, HHS

Release Date
Aug 08, 2024 (UTC)

Alert ID 37c9be32

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags CVE-2024-37287, Kibana, ElasticSearch

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**