|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |
| --- |
|   |

A close-up of a logo  AI-generated content may be incorrect.

|  |
| --- |
|   |

 |  |

 |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
|   |

**Vulnerability Bulletins** |  |

 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
|   |

**Elastic Patches Critical Kibana Flaw CVE-2025-25015**

|  |
| --- |
|   |

 |

 |

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|   |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |
| --- |
| A white circle on a gray background  AI-generated content may be incorrect. |

 |

|  |
| --- |
| TLP:WHITE  |

 |

 |

 |

|  |
| --- |
| Mar 07, 2025 |

 |

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |
| --- | --- |
|

|  |
| --- |
| On March 5, 2025, Elastic [released](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdiscuss.elastic.co%2Ft%2Fkibana-8-17-3-security-update-esa-2025-06%2F375441&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933177517%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=FgvkQzMxNEYtqKSRzFhKw1ttNGnJZH3fTKy3oQXOyFI%3D&reserved=0) a security update to fix a critical vulnerability in Kibana, data visualization dashboard software. The flaw tracked as CVE-2025-25015 has a CVSS score of 9.9, highlighting its criticality. |

 |

|  |  |
| --- | --- |
|

|  |
| --- |
| Kibana is a data visualization tool for Elasticsearch. Elasticsearch is used in the health sector for medical record search, data management, insights, and threat detection.The flaw, CVE-2025-25015, could allow threat actors to send specially crafted files and use specifically crafted HTTP requests to achieve arbitrary code execution. It exists due to prototype pollution and affects all Kibana versions from 8.15.0 to 8.17.3.A prototype pollution flaw is a security issue in which threat actors can manipulate JavaScript objects and properties, potentially leading to various security issues, including remote code execution.Exploitation of CVE-2025-25015 is limited to certain user roles with specific privileges in vulnerable versions. For example, in Kibana versions 8.15.0 to 8.17.1, vulnerability affects users with the enabled viewer role. In other vulnerable versions like 8.17.1 and 8.17.2, the exploitation requires fleet-all, integrations-all, and actions:execute-advanced-connectors privileges.Health-ISAC advises users to patch vulnerable Elastic instances immediately. Those unable to patch should disable the conditions required for exploitation depending on the vulnerable version.**Recommendations:*** Apply available patches for vulnerable devices.
* Enforce network segmentation and strict network access control policies.
* Implement multi-factor authentication for accounts across the organization.
* Continuously monitor for suspicious activities.
* Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
* Review the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients resources](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2F405d.hhs.gov%2FDocuments%2FHICP-Main-508.pdf&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933200035%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=P4bxRk1JUAFNTqlgvxw%2BRYB5orgTEVacPYpE9nIhATY%3D&reserved=0).

  |

 |

 |

 |

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|   |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |
| --- |
| **Reference(s)**  |

 |

|  |
| --- |
| [The Hacker News](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fthehackernews.com%2F2025%2F03%2Felastic-releases-urgent-fix-for.html&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933211615%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=5iGP5xQ1coaQZawHIjx4YPY2PMAFN1X5ogOJ0hXsNDs%3D&reserved=0), [HHS](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2F405d.hhs.gov%2FDocuments%2FHICP-Main-508.pdf&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933223083%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=k0pLWHKu9pWKplAlBZBN0KHoONnsPyYvGv%2FoD9hSU5M%3D&reserved=0), [Elastic](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdiscuss.elastic.co%2Ft%2Fkibana-8-17-3-security-update-esa-2025-06%2F375441&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933234358%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=9rpIHcXCy4QA2ylwFcbiH94aMkiu34xYCYx1OleqFIg%3D&reserved=0), [Security Affairs](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsecurityaffairs.com%2F174999%2Fsecurity%2Felastic-kibana-critical-flaw.html&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933245500%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=EDeNSFkotvRFqbFvicU%2B%2BZBeRa93WkS%2BbfSsmzhynD8%3D&reserved=0)  |

 |

 |

 |

|  |
| --- |
|  |

 |

 |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|   |

**Sources**

|  |  |
| --- | --- |
|

|  |
| --- |
| [https://discuss.elastic.co/t/kibana-8-17-3-security-update-esa-2025-06/375441](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdiscuss.elastic.co%2Ft%2Fkibana-8-17-3-security-update-esa-2025-06%2F375441&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933256642%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=9xvIQHY6YzReYmfjaq9RSOm%2Bq%2B6gW%2BxN2hson0bpYgQ%3D&reserved=0)[https://thehackernews.com/2025/03/elastic-releases-urgent-fix-for.html](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fthehackernews.com%2F2025%2F03%2Felastic-releases-urgent-fix-for.html&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933268212%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=F9ngi7Xtqw8krO6p%2FBXRy3G4WZSVG1h9WwSrrIxqrqE%3D&reserved=0)<https://securityaffairs.com/174999/security/elastic-kibana-critical-flaw.html> |

 |

**Release Date**

|  |  |
| --- | --- |
|

|  |
| --- |
| Mar 07, 2025 (UTC) |

 |

|  |
| --- |
|   |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| **Alert ID** 3ba8d8a2  |  |
|  |  |

 |

|  |
| --- |
|  |

 |

 |

 |

 |

 |

|  |
| --- |
|  |

 |

|  |
| --- |
|  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|   |

|  |
| --- |
|   |

[**View Alert**](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fhealth-isac.cyware.com%2Fwebapp%2Fuser%2Fmyfeeds%2F3ba8d8a2&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933279490%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=%2BoSrPTizfHpt81s57xIusFteTC0QQX66UTh%2B5lugpoE%3D&reserved=0)Share Feedbackwas this helpful? Like |  Dislike

|  |
| --- |
|   |

|  |  |
| --- | --- |
|

|  |
| --- |
| **Tags** CVE-2025-25015, 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/**](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fhealth-isac.cyware.com%2Fwebapp%2F&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933337613%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=EMs%2BmsPQcHoXo7pQrtYEGd2zhWp6k9QnvqMYnnRm7wI%3D&reserved=0)  |

 |

|  |
| --- |
|  |

 |

|  |  |
| --- | --- |
|

|  |
| --- |
|  |

 |

|  |
| --- |
|   |

 |

 |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
|   |

If you are not supposed to receive this email,please contact us at **toc@h-isac.org**.  |  |

 |

 |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
|   |

Powered by [Cyware](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcyware.com%2F&data=05%7C02%7Cdsamuels%40aha.org%7Cb0200f3ecc38421d2a2b08dd5d6bd5ec%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C0%7C638769439933349959%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=1BxCMkwKDYoWjEZOBMm3pENyJEi1ffcyJLae%2BibjqHI%3D&reserved=0)  |  |

 |

|  |
| --- |
|   |

 |