网络安全预警通报

2025 年第 2 期 （总第 52 期）

西安交通大学网络信息中心 2025 年 3 月 10 日

【预警类型】高危预警

【预警内容】

Elastic Kibana 存在任意代码执行漏洞

一、漏洞概述

Elastic Kibana 平台中存在高危任意代码执行漏洞 CVE-2025-25012（漏洞评分 9.9），攻击者可通过精心设计的文件上传和特制的 HTTP 请求执行任意代码，获取服务器敏感数据，进而控制整服务器。

二、漏洞详情

Kibana 是一个广泛用于可视化和探索存储在 Elasticsearch 中的数据的可视化和探索平台。Kibana 为 Elasticsearch 集群上索引的内容提供可视化功能。用户可以在大量数据上创建条形图、折线图和散点图，或饼图和地图。

据描述，该漏洞源于原型污染问题，攻击者可通过精心设计的文件上传和特制的 HTTP 请求执行任意代码，获取服务器敏感数据，进而控制整服务器。

三、漏洞影响范围

漏洞影响的产品和版本：

Kibana versions>=8.15.0 and <8.17.3

在 Kibana 版本 8.15.0 至 8.17.0：可由具有“viewer”权限的角色可利用。

在 Kibana 版本 8.17.1 和 8.17.2 中只有拥有包含以下所有权限的角色才能利用此漏洞：fleet-all、integrations-all 以及 actions:execute-advanced-connectors

四、漏洞缓解措施

1.临时缓解措施

禁用 Integration Assistant 功能，修改配置文件参数值如下：

xpack.integration_assistant.enabled：false

2．升级修复

Elastic Kibana 8.17.3 版本已解决 CVE-2025-25012 漏洞，并强烈敦促所有用户尽快升级到此版本。