态势感知设备是否涉及Elasticsearch 服务器存在未授权访问漏洞

漏洞相关 **王树岭** 2022-07-22 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： Elasticsearch 服务器存在未授权访问漏洞

产品型号及版本： 态势感知系列（csap、csap-sa）

漏洞描述

Elasticsearch 是一个开源的高扩展的分布式全文检索引擎，它可以近乎实时的存储、 检索数据；本身扩展性很好，可以扩展到上百台服务器，处理PB 级别的数据。Elastic search 也使用Java 开发并使用Lucene 作为其核心来实现所有索引和搜索的功能，但 是它的目的是通过简单的RESTful API 来隐藏Lucene 的复杂性，从而让全文搜索变得 简单。ElasticSearch 是一款Java 编写的企业级搜索服务，启动此服务默认会开放HTTP -9200 端口，可被非法操作数据。

处置建议 方案一：限制IP 访问，禁止未授权IP 访问ElasticSearch 端口(默认9200)。 方案二：通过ES 插件形式来增加访问验证，需要注意增加验证后切勿使用弱

漏洞解决方案

态势感知系列未开放该端口（9200），不涉及该漏洞