# **漏洞报告**

###### **漏洞编号**

CVE-2021-22147

###### **漏洞描述**

###### 在 Elasticsearch 中发现了一个缺陷，即文档和字段级安全性未应用于可搜索快照。这可能会导致经过身份验证的用户访问他们未经授权查看的信息。

###### **漏洞来源**

平台：CVE/NVD 链接：[NVD - CVE-2021-22147 (nist.gov)](https://nvd.nist.gov/vuln/detail/CVE-2021-22147)

###### **漏洞披露时间**

###### 2021-08-03

###### **漏洞参考链接**

[Elastic Stack 7.14.0 Security Update](https://discuss.elastic.co/t/elastic-stack-7-14-0-security-update/280344): [Elastic Stack 7.14.0 Security Update - Announcements / Security Announcements - Discuss the Elastic Stack](https://discuss.elastic.co/t/elastic-stack-7-14-0-security-update/280344?utm_source=feedly)

Red Hat: [CVE-2021-22147- Red Hat Customer Portal](https://access.redhat.com/security/cve/cve-2021-22147)

###### **野外漏洞报告**

SUSE: <https://www.suse.com/fr-fr/security/cve/CVE-2021-22147.html>

###### **漏洞类型**

CWE-862,CWE-732

###### **漏洞危害**

###### 在Elastic App Search中发现了一个缺陷，即 API 密钥缺少通过备用路由的授权。利用此漏洞，经过身份验证的攻击者可以利用属于更高权限用户的 API 密钥。

###### **漏洞严重性**

NVD: CVSS Version 3.x: 6.5 MEDIUM; CVSS Version 2.0:4.0 MEDIUM

SUSE:CVSS Version 3.x: 5.7

###### **漏洞影响的组件版本**

Elasticsearch versions 7.11.0 to 7.13.4

###### **漏洞修复的组件版本**

Elasticsearch 7.14.0及以后的版本

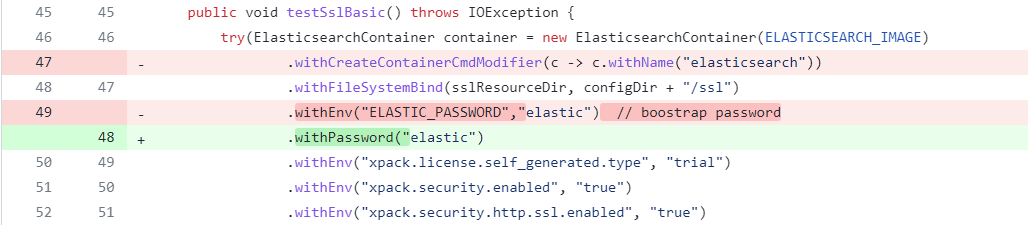
**漏洞成因**

在7.14.0 之前的 Elasticsearch 没有对可搜索快照应用文档和字段级别的安全性。这可能会导致经过身份验证的用户获得对他们无权查看的信息的访问权限。

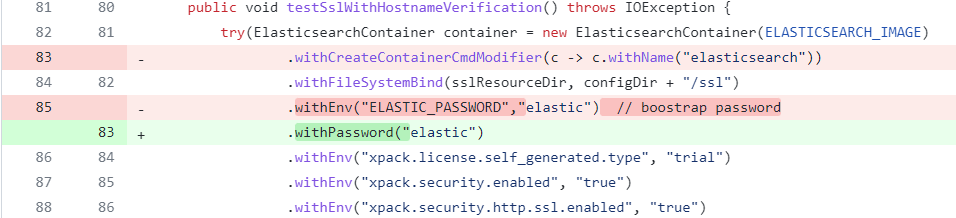
###### **漏洞位置**

<https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b#diff-4516062fd37f01febd984641f4312707d17871dc915b6c0be39118ba2325ee03>

函数：testSslBasic() 位置：第45-51行

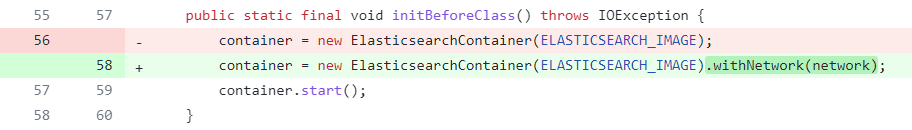


函数：testSslWithHostnameVerification() 位置：第80-86行

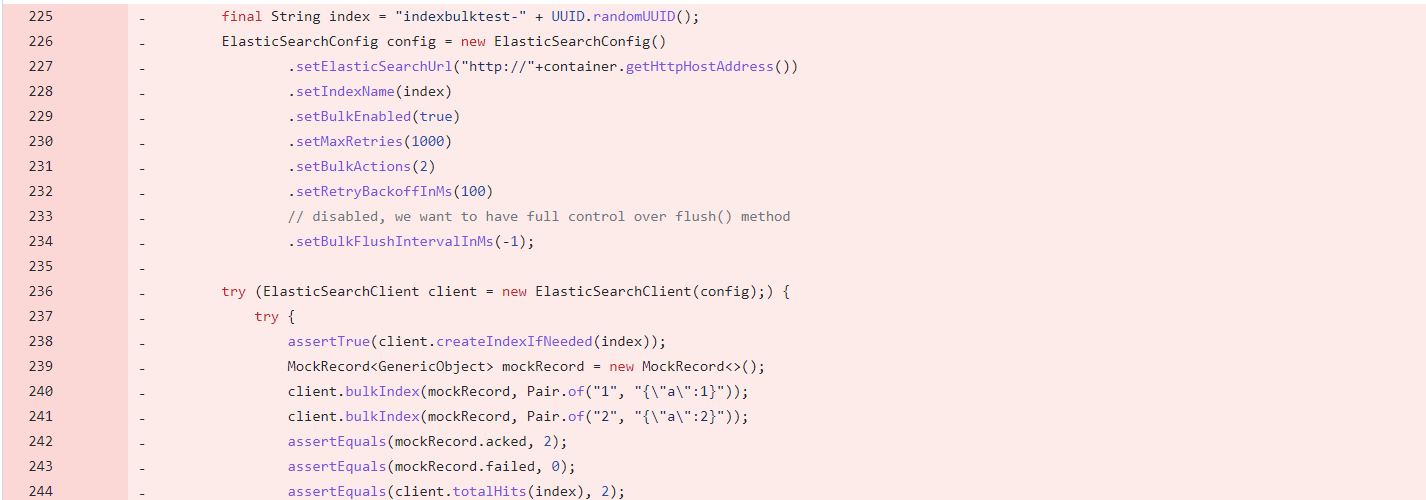


<https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b#diff-2c290af7e0a5d1818a605d706015f362e5d9705c74b5d3764038e7f2f278d6e7>

函数：initBeforeClass() 位置：第57-60行



函数：testBulkRetry() 位置：第225-260行







###### **漏洞PoC**

暂无

###### **漏洞补丁**

<https://github.com/gridgentoo/pulsar/commit/1af8d3fc6bca31c1ca059a2dda80e6d8eb7ae24b>

###### **漏洞处置建议**

用户应升级Elasticsearch到版本 7.14.0