Security Advisory Report - OBSO-1904-01

Elasticsearch Improper Permissions Name Indexing Remote Privilege Escalation (CVE-2019-7611)

Release Date: 2019-04-25 12:25:04
Last Update: 2019-04-25 12:27:29

Summary

A permission issue was found in Elasticsearch when Field Level Security and Document Level Security are disabled and the _aliases, _shrink, or _split endpoints are used.
If the elasticsearch.yml file has xpack.security.dls_fls.enabled set to false, certain permission checks are skipped when users perform one of the actions mentioned above, to make existing data available under a new index/alias name. This could result in an attacker gaining additional permissions against a restricted index.

Risk rate: medium

Details

Elasticsearch improper permission issue when attaching a new name to an index (ESA-2019-04)

Elasticsearch contains a flaw that is triggered as certain permission checks are not properly performed if the elasticsearch.yml file has xpack.security.dls_fls.enabled set to false. This may allow an **authenticated remote attacker** to potentially gain elevated privileges.

This vulnerability is only relevant when Field Level Security and Document Level Security are disabled and the _aliases, _shrink, or _split endpoints are in use.

Affected Versions
Elasticsearch Security versions before 5.6.15 and 6.6.1

Solutions and Mitigations:
Users should upgrade to Elasticsearch version 6.6.1 or 5.6.15. Users unable to upgrade can change the xpack.security.dls_fls.enabled setting to true in their elasticsearch.yml file.
The default setting for this option is true.

https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077

CVE ID: CVE-2019-7611

Affected Products

Not affected products:

Circuit Access Node
Circuit Application Node
Circuit Load Balancer Node
Circuit Management Node
Circuit Operations Node
Circuit Provisioning Engine Node
Circuit Storage Node
Circuit Storage Node
Circuit XMPP Gateway Node
Circuit Zookeeper Node

Contact Center

Affected products:

OpenScape Composer is affected with low priority. Fix is in work

All other products do not use Elasticsearch

Recommended Actions

Update OpenScape Composer, when the fix is available.

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-7611

https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077

https://www.elastic.co/products/elasticsearch

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com