

nicolargo / glances Public

<> Code Issues 90 Pull requests 12 Discussions Actions Projects

# Commit d339181

 morimori-dev committed 2 weeks ago · ✖ 2 / 3

fix(cassandra): validate keyspace/table/replication\_factor to prevent CQL injection

Interpolating config values directly into CQL strings allows an attacker with write access to glances.conf to inject arbitrary CQL statements via the keyspace, table, or replication\_factor fields.

Add \_validate\_cql\_identifier() to enforce that keyspace and table contain only letters, digits, and underscores (standard CQL identifier rules). Cast replication\_factor to int and reject values less than 1.

Fixes [GHSA-grp3-h8m8-45p7](#) / CVE-2026-35588

 develop (#3520) ·  v4.5.4


1 parent [8aa6137](#) commit d339181 

 1 file changed +25 -0 lines changed


↑ Top 

🔍 Filter files... 

✓  glances/exports/glances\_cassandra

 \_\_init\_\_.py

 1 file changed +25 -0 lines changed

🔍 Search within code 

```

glances/exports/glances_cassandra/__init__.py
...
@@ -8,6 +8,7 @@
8 8
9 9     """Cassandra/Scylla interface class."""
10 10
11 + import re
11 12     import sys

```

```

12 13     from datetime import datetime
13 14     from numbers import Number
@@ -21,6 +22,19 @@
21 22     from glances.logger import logger
22 23
23 24
25 + _CQL_IDENTIFIER_RE = re.compile(r'^[a-zA-Z][a-zA-Z0-9_]*$')
26 +
27 +
28 + def _validate_cql_identifier(value, name):
29 +     """Raise ValueError if value is not a safe CQL identifier."""
30 +     if not _CQL_IDENTIFIER_RE.match(str(value)):
31 +         raise ValueError(
32 +             f"Invalid CQL identifier for '{name}': {value!r}. "
33 +             "Only letters, digits, and underscores are allowed, and it must
34 +             start with a letter."
35 +         )
36 +     return str(value)
37 +
24 38     class Export(GlancesExport):
25 39         """This class manages the Cassandra/Scylla export module."""
26 40
@@ -47,6 +61,17 @@ def __init__(self, config=None, args=None):
47 61         if not self.export_enable:
48 62             sys.exit(2)
49 63
64 +         # Validate CQL identifiers to prevent injection via config values
65 +         try:
66 +             self.keyspace = _validate_cql_identifier(self.keyspace, 'keyspace')
67 +             self.table = _validate_cql_identifier(self.table, 'table')
68 +             self.replication_factor = int(self.replication_factor)
69 +             if self.replication_factor < 1:
70 +                 raise ValueError("replication_factor must be a positive
71 +                 integer")
72 +             except ValueError as e:
73 +                 logger.critical(f"Cassandra configuration error: {e}")
74 +                 sys.exit(2)
50 75         # Init the Cassandra client

```

```
51     76         self.cluster, self.session = self.init()
```

```
52     77
```



## Comments 0



Please [sign in](#) to comment.