nicolargo / **glances** Public

Code Issues 90 Pull requests 12 Discussions Actions Projects

Commit e41b665

nicolargo authored last week · ✕ 2 / 11 · Verified

```
Merge pull request #3520 from morimori-dev/fix/cassandra-cql-injection-GHSA-grp3-h8m8-45p7

fix(cassandra): validate keyspace/table/replication_factor to prevent CQL injection (GHSA-grp3-h8m8-45p7)
```

develop (#3520) · v4.5.4

2 parents 24615e5 + 1563ff8 commit e41b665

1 file changed +26 -0 lines changed

Top

Filter files…

glances/exports/glances_cassandra

__init__.py

1 file changed +26 -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
        start with a letter."
    34  +         )
    35  +     return str(value)
    36  +
    37  +
24  38    class Export(GlancesExport):
25  39        """This class manages the Cassandra/Scylla export module."""
26  40
        @@ -47,6 +61,18 @@ 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
        integer")
    71  +         except ValueError as e:
    72  +             logger.error(f"Cassandra configuration error: {e}")
    73  +             self.export_enable = False
    74  +             return
    75  +
50  76            # Init the Cassandra client
51  77            self.cluster, self.session = self.init()
52  78
```

Comments 0

Please sign in to comment.