Passwords used to access external services inadvertently exposed through API

Moderate julianbrost published GHSA-wrpw-pmr8-qgj7 on Jul 15, 2021

Package

No package listed

Affected versions	Patched versions
< 2.11.10, 2.12.0 to 2.12.4	2.11.10, 2.12.5

Description

Impact

Some of the Icinga 2 features that require credentials for external services exposed those through the API. The following features inadvertently exposed these credentials to authenticated API users with read permissions for the corresponding object types:

- *IdoMysqlConnection* and *IdoPgsqlConnection* (every released version): password of the user used to connect to the database
- *IcingaDB* (added in 2.12.0): password used to connect to the Redis server
- *ElasticsearchWriter* (added in 2.8.0): password used to connect to the Elasticsearch server

An attacker who obtained these credentials can impersonate Icinga to these services and add, modify and delete information there. If credentials with more permissions are in use, this increases the impact accordingly.

Patches

Starting with the 2.11.10 and 2.12.5 releases, these passwords are no longer exposed via the API.

Workarounds

API user permissions can be restricted to not allow querying of any affected objects. Either by explicitly listing only the required object types for object query permissions:

```
object ApiUser "example" {
  password = "secret"
  permissions = [ "objects/query/Host", "objects/query/Service" ]
}
```

Or by applying a filter rule:

```
object ApiUser "example" {
  password = "secret"
  permissions = [ {
    permission = "objects/query/*"
    filter = {{ ! ["IdoMysqlConnection", "IdoPgsqlConnection", "IcingaDB", "ElasticsearchWriter"].contains(obj.type) }}
  } ]
}
```

References

- https://icinga.com/blog/2021/07/15/releasing-icinga-2-12-5-and-2-11-10/

For more information

If you have any questions or comments about this advisory:

- Email us at security@icinga.com

Severity

Moderate

CVE ID

CVE-2021-32743

Weaknesses

No CWEs