Custom variable protection and blacklists can be circumvented

Moderate **nilmerg** published **GHSA-2xv9-886q-p7xx** on Jul 12, 2021

Package

No package listed

Affected versions

2.0.0 to 2.8.2

Patched versions

2.7.5, 2.8.3 and 2.9.0

Description

Impact

Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked.

Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user.

Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter on the following routes:

- `/icingaweb2/monitoring/list/hosts`
- `/icingaweb2/monitoring/list/services`

By adding the `?addColumns=_host_secret,_service_secret` parameter to them, Icinga Web 2 will show these columns additionally in the respective list. This parameter is also respected when exporting to JSON or CSV.

Protection rules and blacklists however have no effect in this case. **Custom variables are shown as-is in the result.**

Patches

The issue has been fixed in the v2.7.5, v2.8.3 and v2.9.0 releases.

Workarounds

Setup a restriction to hide hosts and services with the custom variable in question. (e.g. `host_name!=host-with-secrets&service_description!=service-with-secrets`)

References

None.

Severity

Moderate

CVE ID

CVE-2021-32747

Weaknesses

No CWEs