ja4: invalid alpn leads to panic

High **victorjulien** published **GHSA-w5xv-6586-jpm7** on Oct 16, 2024

Package

suricata

Affected versions

< 7.0.7

Patched versions

7.0.7

Description

Impact

Invalid ALPN in TLS/QUIC traffic when JA4 matching/logging is enabled can lead to Suricata aborting with a panic.

Patches

This issue has been addressed in 7.0.7.

Workarounds

JA4 is used in TLS and QUIC, and each is handled separately.

TLS

JA4 for TLS can be disabled in the `tls` section of the `app-layer` configuration by setting `ja4-fingerprints` to `false` (default: `auto`). For example:

```
app-layer:
  tls:
    ja4-fingerprints: false
```

Quic

Quic does not have a JA4 feature flag and it is always enabled, so the recommendation is to disable Quic until Suricata can be updated, for example:

```
app-layer:
  quic:
    enabled: false
```

References

https://redmine.openinfosecfoundation.org/issues/7267

Credits

Found by OSS-fuzz.

Severity

High 7.5 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2024-47522

Weaknesses

▶ CWE-617