defrag: off by one can lead to policy bypass

Moderate **victorjulien** published **GHSA-mf6r-3xp2-v7xg** on Oct 16, 2024

Package

suricata

Affected versions

< 7.0.7

Patched versions

7.0.7

Description

Impact

A logic error during fragment reassembly can lead to failed reassembly for valid traffic. An attacker could craft packets to trigger this behavior.

Patches

This issue has been addressed in 7.0.7.

References

https://redmine.openinfosecfoundation.org/issues/7067

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None

User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2024-45796

Weaknesses

▶ CWE-193