



# CVE-2018-1000167

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-1000167
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-18 19:29:00 UTC
<b>Updated</b>	2018-05-22 16:01:00 UTC
<b>Description</b>	OISF suricata-update version 1.0.0a1 contains an Insecure Deserialization vulnerability in the insecure yaml.load-Function

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Oisf</a>	<a href="#">Suricata-update</a>	1.0.0a1	All	All	All
Application	<a href="#">Oisf</a>	<a href="#">Suricata-update</a>	1.0.0a1	All	All	All

## References

Reference	Source	Link
Remote-Code-Execution in Suricata-Update   FyhTech	MISC	<a href="#">tech.fe</a>
Bug #2359: (Remote)Code-Execution while reading yaml-file - Suricata-Update - Open Information Security Foundation	MISC	<a href="#">redmir</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[997548](#) Python (Pip) Security Update for suricata-update (GHSA-7c4h-w765-6pwg)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**