



CVE-2010-3300

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2010-3300 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-06-22 12:15:00 UTC |
| Updated | 2021-06-25 17:38:00 UTC |
| Description | It was found that all OWASP ESAPI for Java up to version 2.0 RC2 are vulnerable to padding oracle attacks. |

Risk And Classification

Problem Types: CWE-649

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------------------|--|---------|--------|---------|----------|
| Application | Owasp | Enterprise Security Api For Java | All | All | All | All |
| Application | Owasp | Enterprise Security Api For Java | 2.0 | - | All | All |
| Application | Owasp | Enterprise Security Api For Java | 2.0 | rc1 | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|---------------------|
| www.usenix.org/legacy/events/woot10/tech/full_papers/Rizzo.pdf | MISC | www.usenix.org | |
| oss-sec: Re: CVE request: padding oracle attack: ruby on rails 2.3, owasp esapi | MISC | seclists.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981708](#) Java (maven) Security Update for org.owasp.esapi:esapi (GHSA-3gp6-hhfw-4gqx)

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](#)