



# CVE-2015-3216

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

## Summary

<b>CVE</b>	CVE-2015-3216
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-07-07 10:59:00 UTC
<b>Updated</b>	2018-01-05 02:30:00 UTC
<b>Description</b>	Race condition in a certain Red Hat patch to the PRNG lock implementation in the <code>ssleay_rand_bytes</code> function in OpenSSL

## Risk And Classification

**Problem Types:** CWE-189 | CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1e-25.el7	All	All	All
Application	<a href="#">Openssl</a>	<a href="#">Openssl</a>	1.0.1e-25.el7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All

## References

Reference	Source	Link
Red Hat OpenSSL Locking Error in <code>ssleay_rand_bytes()</code> Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytra.com">www.securitytra.com</a>
[security-announce] SUSE-SU-2015:1143-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
[security-announce] SUSE-SU-2015:1182-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
[security-announce] SUSE-SU-2015:1184-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
[security-announce] SUSE-SU-2015:1150-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
OpenSSL ' <code>ssleay_rand_bytes()</code> ' Function Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
Bug 1225994 – segfault in <code>ssleay_rand_bytes</code> due to locking regression	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
[security-announce] openSUSE-SU-2015:1139-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>
<p>No vendor comments have been submitted for this CVE.</p>		
<h3>Legacy QID Mappings</h3>		
<p><a href="#">390226</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)</p>		
<p><a href="#">390284</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)</p>		

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)