



# CVE-2011-0343

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

## Summary

<b>CVE</b>	CVE-2011-0343
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-01-28 16:00:00 UTC
<b>Updated</b>	2020-05-19 19:30:00 UTC
<b>Description</b>	Balabit syslog-ng 2.0, 3.0, 3.1, 3.2 OSE and PE, when running on FreeBSD or HP-UX, does not properly perform cast oper

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	All	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Hp-ux</a>	All	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Hp-ux</a>	All	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	2.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	2.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.1	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.1	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.2	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.2	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	2.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	2.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.0	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.1	All	All	All

Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.1	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.2	All	All	All
Application	<a href="#">Oneidentity</a>	<a href="#">Syslog-ng</a>	3.2	All	All	All

## References

Reference	Source	Link	Tag
[syslog-ng-announce] syslog-ng Premium Edition 3.2.1a has been released	MLIST	<a href="https://lists.balabit.com">lists.balabit.com</a>	Ven
syslog-ng Insecure File Permissions Local Privilege Escalation Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Thir
SecurityFocus	BUGTRAQ	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Thir
[syslog-ng-announce] syslog-ng Premium Edition 3.0.6a has been released	MLIST	<a href="https://lists.balabit.com">lists.balabit.com</a>	Ven
#608491 - syslog-ng: log file permissions dangerous on kfreebsd-i386 - Debian Bug report logs	CONFIRM	<a href="https://bugs.debian.org">bugs.debian.org</a>	Patc
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://status.cve.report)**