



# CVE-2016-7406

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

## Summary

<b>CVE</b>	CVE-2016-7406
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-03 16:59:00 UTC
<b>Updated</b>	2017-03-04 23:00:00 UTC
<b>Description</b>	Format string vulnerability in Dropbear SSH before 2016.74 allows remote attackers to execute arbitrary code via format str

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dropbear Ssh Project	Dropbear Ssh	All	All	All	All

## References

### Reference

- oss-security - Re: CVE request for Dropbear SSH <2016.74
- 1376353 – (CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409) CVE-2016-7406 CVE-2016-7407 CVE-2016-7408 CVE-2016-7409
- dropbear: b66a483f3dcb
- Dropbear: Multiple vulnerabilities (GLSA 201702-23) — Gentoo Security
- Dropbear SSH CVE-2016-7406 Format String Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710451](#) Gentoo Linux Dropbear Multiple Vulnerabilities (GLSA 201702-23)

© [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](#)**