



# CVE-2006-3567

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

## Summary

<b>CVE</b>	CVE-2006-3567
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-07-13 01:05:00 UTC
<b>Updated</b>	2018-10-18 16:48:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the web administration interface logging feature in Juniper Networks (Redline) DX

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Juniper	Dx	All	All	All	All

## References

### Reference

Juniper Networks DX System Log Script Insertion - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityFocus
Juniper Networks DX Web Login HTML Injection Vulnerability
27131
CXSecurity - IDS
IBM X-Force Exchange
SecurityTracker.com Archives - Juniper DX Application Acceleration Platform Input Validation Hole in Web Interface Permits Cross-Site Script
CVE Program record
NVD vulnerability detail

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](#)**