



# CVE-2010-0387

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

## Summary

<b>CVE</b>	CVE-2010-0387
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-01-25 19:30:00 UTC
<b>Updated</b>	2017-08-17 01:31:00 UTC
<b>Description</b>	Multiple heap-based buffer overflows in (1) webservd and (2) the admin server in Sun Java System Web Server 7.0 Update

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sun	Java System Web Server	7.0	update_7	All	All
Application	Sun	Java System Web Server	7.0	update_7	All	All

## References

### Reference

Sun Java System Web Server Digest Authentication Remote Buffer Overflow Vulnerability
[Dailydave] Sun Web Server digest auth overflow
IBM X-Force Exchange
intevydis security research
Sun Java System Web Server Heap Overflow in Processing HTTP Digest Authentication Requests Lets Remote Users Execute Arbitrary Code
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](#)**