



# CVE-2012-3007

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2012-3007
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-07-05 03:23:18 UTC
<b>Updated</b>	2026-04-29 01:13:23 UTC
<b>Description</b>	Stack-based buffer overflow in slssvc.exe before 58.x in Invensys Wonderware SuiteLink in the Invensys System Platform s

## Risk And Classification

**Primary CVSS:** v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

**Problem Types:** CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Invensys	Dasabcip	4.1	All	All	All

Application	<a href="#">Invensys</a>	<a href="#">Dasabcip</a>	All	sp1	All	All
Application	<a href="#">Invensys</a>	<a href="#">Daserver Runtime Components</a>	3.0	All	All	All
Application	<a href="#">Invensys</a>	<a href="#">Daserver Runtime Components</a>	All	sp1	All	All
Application	<a href="#">Invensys</a>	<a href="#">Dassidirect</a>	All	All	All	All
Application	<a href="#">Invensys</a>	<a href="#">Intouch/wonderware Application Server</a>	All	All	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	3.0	All	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	3.0.200	sp2	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	3.1	All	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	3.1	sp1	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	3.1.201	sp2	All	All
Application	<a href="#">Invensys</a>	<a href="#">Wonderware Application Server</a>	All	sp2	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

Reference	Source
Wonderware SuiteLink Unallocated Unicode String Remote Denial of Service Vulnerability	af854a3a-2127-42
404 - File Not Found   CISA	af854a3a-2127-42
Security Advisory SA49173 - Invensys Wonderware InTouch SuiteLink Service Denial of Service Vulnerability - Secunia	af854a3a-2127-42
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free **CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)