



CVE-2011-0488

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

Summary

CVE	CVE-2011-0488
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-18 18:03:09 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in NTWebServer.exe in the test web service in InduSoft NTWebServer, as distributed in Advan

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Advantech Studio	6.1	All	All	All

Application	Indusoft	Web Studio	7.0	All	All	All
-------------	----------	------------	-----	-----	-----	-----

Vendor Declared Affected Products

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

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Advantech Studio NTWebServer Buffer Overflow and Directory Traversal Vulnerabilities - Secunia.com
IBM X-Force Exchange
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
InduSoft NTWebServer Web Service Stack-Based Buffer Overflow Vulnerability
InduSoft Web Studio NTWebServer Buffer Overflow and Directory Traversal Vulnerabilities - Secunia.com
404 - File Not Found CISA
www.osvdb.org/70396
Advantech Studio Test Web Server Buffer Overflow Notice
downloadt.advantech.com/download/downloadsr.aspx
InduSoft – HMI SCADA Supervisory Software PLC OPC Web Database Connectivity » Blog Archive » SCADA Security Reminder for InduSoft
US-CERT Vulnerability Note VU#506864 - InduSoft NTWebServer web service stack-based buffer overflow
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](#).

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

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