InduSoft Web Studio Path Traversal

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0780
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-25 05:12:07 UTC
Updated	2026-04-22 16:07:06 UTC
Description	Directory traversal vulnerability in NTWebServer in InduSoft Web Studio 7.1 before SP2 Patch 4 allows remote attackers to

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.892470000 probability, percentile 0.995430000 (date 2026-04-30)

CISA KEV: Listed on 2022-04-15; due 2022-05-06; ransomware use Unknown

Problem Types: CWE-22 | CWE-22 CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	ics-cert@hq.dhs.gov	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	CVSS	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

CISA Known Exploited Vulnerability

Vendor	InduSoft
Product	Web Studio
Name	InduSoft Web Studio NTWebServer Directory Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-0780

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Indusoft	Web Studio	7.1	-	All	All
Application	Indusoft	Web Studio	7.1	sp1	All	All
Application	Indusoft	Web Studio	7.1	sp2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	InduSoft	Web Studio	affected 7.1	Not specified

References

Reference	Source	Link
InduSoft Web Studio CVE-2014-0780 Directory Traversal Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfoc
www.cisa.gov/news-events/ics-advisories/icsa-14-107-02	ics-cert@hq.dhs.gov	www.cisa.gov
Indusoft Web Studio - Directory Traversal Information Disclosure (Metasploit)	af854a3a-2127-422b-91ae-364da2661108	www.exploit-db.c
download.indusoft.com/71.2.4/IWS71.2.4.zip	ics-cert@hq.dhs.gov	download.indusc
InduSoft Web Studio Directory Traversal Vulnerability | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cert.us-cert.g
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

Vendor Comments And Credit

Discovery Credit

CNA: Zero Day Initiative (ZDI) (en)

Additional Advisory Data

Source	Time	Event
ADP	2022-04-15T00:00:00.000Z	CVE-2014-0780 added to CISA KEV

Solutions

CNA: InduSoft did not intend for this web server to be used in real applications. It was provided as demonstration/training software (as stated in user manuals). They have created a mitigation for this vulnerability in InduSoft Web Studio v7.1+Service Pack 2+ Patch 4. Users may obtain this patch at the following location (you must be logged into your InduSoft account): http://download.indusoft.com/71.2.4/IWS71.2.4.zip InduSoft technical support can be contacted at: support@indusoft.com .

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report