



Ecava IntegraXor Exposure of Access Control List Files to an Unauthorized Control Sphere

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

Summary

CVE	CVE-2014-0752
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-09 18:07:26 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SCADA server in Ecava IntegraXor before 4.1.4369 allows remote attackers to read arbitrary project backup files via a

Risk And Classification

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

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

EPSS: 0.025620000 probability, percentile 0.855810000 (date 2026-04-30)

Problem Types: CWE-529 | CWE-264 | CWE-529 CWE-529

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N
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 v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ecava	Integraxor	3.5.3900.10	All	All	All
Application	Ecava	Integraxor	3.5.3900.5	All	All	All
Application	Ecava	Integraxor	3.6.4000.0	All	All	All
Application	Ecava	Integraxor	3.60.4061	All	All	All
Application	Ecava	Integraxor	3.71	All	All	All
Application	Ecava	Integraxor	3.71.4200	All	All	All
Application	Ecava	Integraxor	3.72	All	All	All
Application	Ecava	Integraxor	4.00	All	All	All
Application	Ecava	Integraxor	4.1	All	All	All
Application	Ecava	Integraxor	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ecava	IntegraXor	affected 4.1.4360 custom	Not specified

References

Reference	Source	
IntegraXor HMI/SCADA • Free Web SCADA for 128 Modbus I/O	af854a3a-2127-422b-91ae-364da2661108	vulnerability details
www.cisa.gov/news-events/ics-advisories/icsa-14-008-01	ics-cert@hq.dhs.gov	vulnerability details
Ecava Sdn Bhd IntegraXor Project Directory Information Disclosure Vulnerability ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cert.org
CVE Program record	CVE.ORG	vulnerability details
NVD vulnerability detail	NVD	vulnerability details

Vendor Comments And Credit

Discovery Credit

CNA: Zero Day Initiative (en)

Additional Advisory Data

Solutions

CNA: Ecava Sdn Bhd has issued a customer notification that details this vulnerability and

provides mitigations to its customers. Ecava Sdn Bhd recommends users download and install the update, IntegraXor SCADA Server 4.1.4369, from their support Web site: <http://www.integraxor.com/download/beta.msi?4.1.4369> For additional information, please see Ecava's vulnerability note: <http://www.integraxor.com/blog/category/security/vulnerability-note/>

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](#)