



CVE-2010-4597

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

Summary

CVE	CVE-2010-4597
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-23 18:00:00 UTC
Updated	2011-01-11 06:46:00 UTC
Description	Stack-based buffer overflow in the save method in the IntegraXor.Project ActiveX control in igcomm.dll in Ecava IntegraXor

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ecava	Integraxor	All	All	All	All

References

Reference	Source	Link
SCADA Developer Network » Blog Archive » IntegraXor 3.5 SCADA Security Issue 20101006-0109 Vulnerability Note	MISC	www
Ecava IntegraXor Remote Stack-based Buffer Overflow Vulnerability	BID	www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www
IntegraXor Project ActiveX Control Buffer Overflow Vulnerability - Secunia.com	SECUNIA	secu
Ecava IntegraXor Remote ActiveX Buffer Overflow PoC	EXPLOIT-DB	www
404 - File Not Found CISA	MISC	www
US-CERT Vulnerability Note VU#603928	CERT-VN	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

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](#)