



# CVE-2011-2089

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2011-2089
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-05-13 17:05:00 UTC
<b>Updated</b>	2017-08-29 01:29:00 UTC
<b>Description</b>	Stack-based buffer overflow in the SetActiveXGUID method in the VersionInfo ActiveX control in GenVersion.dll 8.0.138.0 in

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.0	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.01	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.1	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.13	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.2	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.20	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.21	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.0	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.01	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.1	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.13	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.2	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.20	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Bizviz</a>	9.21	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.0	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.01	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.1	All	All	All

Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.13	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.2	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.20	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.21	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.0	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.01	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.1	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.13	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.2	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.20	All	All	All
Application	<a href="#">Iconics</a>	<a href="#">Genesis32</a>	9.21	All	All	All

## References

Reference	Source	Link	Tags
ICONICS WebHMI ActiveX Buffer Overflow	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit
Risks in POS Systems: The Importance of a Security Assessment	MISC	<a href="http://www.security-assessment.com">www.security-assessment.com</a>	Exploit
72135	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>	
ICONICS WebHMI ActiveX Control Stack Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploit
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	Vendor
ICONICS VersionInfo ActiveX Control Buffer Overflow Vulnerability - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
404 - File Not Found   CISA	MISC	<a href="http://www.us-cert.gov">www.us-cert.gov</a>	US Gov
ICONICS WebHMI ActiveX Stack Overflow	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#).

