



CVE-2011-1919

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2011-1919
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-11-02 17:55:00 UTC
Updated	2011-11-17 05:00:00 UTC
Description	Multiple stack-based buffer overflows in GE Intelligent Platforms Proficy Applications before 4.4.1 SIM 101 and 5.x before 5

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ge	Intelligent Platforms Proficy Historian	4.0	All	All	All
Application	Ge	Intelligent Platforms Proficy Historian	5.0	All	All	All
Application	Ge	Intelligent Platforms Proficy Historian	4.0	All	All	All
Application	Ge	Intelligent Platforms Proficy Historian	5.0	All	All	All
Application	Ge	Intelligent Platforms Proficy Historian	All	All	All	All

References

Reference	Source	Link	Tags
GE Proficy Plant Application Components Remote Stack Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	
404 - File Not Found CISA	MISC	www.us-cert.gov	US Go
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	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](#).

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