



CVE-2006-4133

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

Summary

CVE	CVE-2006-4133
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-14 23:04:00 UTC
Updated	2018-10-17 21:33:00 UTC
Description	Heap-based buffer overflow in SAP Internet Graphics Service (IGS) 6.40 and earlier, and 7.00 and earlier, allows remote at

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sap	Internet Graphics Server	6.40	All	All	All
Application	Sap	Internet Graphics Server	6.40_patch_11	All	All	All
Application	Sap	Internet Graphics Server	6.40_patch_15	All	All	All
Application	Sap	Internet Graphics Server	7.00_patch_3	All	All	All
Application	Sap	Internet Graphics Server	6.40	All	All	All
Application	Sap	Internet Graphics Server	6.40_patch_11	All	All	All
Application	Sap	Internet Graphics Server	6.40_patch_15	All	All	All
Application	Sap	Internet Graphics Server	7.00_patch_3	All	All	All

References

Reference
SecurityFocus
SecurityReason - SAP Internet Graphics Service (IGS) Remote Buffer Overflow
SAP Internet Graphics Server Buffer Overflow Lets Remote Users Execute Arbitrary Code and Deny Service - SecurityTracker
VU#259540 - SAP Internet Graphics Service buffer overflow
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Secunia - Advisories - SAP Internet Graphics Service Two Vulnerabilities

SecurityFocus
SAP Internet Graphics Server Remote Buffer Overflow Vulnerability
SAP Internet Graphics Server Buffer Overflow in Processing ADM:GETLOGFILE Command Errors Lets Remote Users Execute Arbitrary Code
www.cybsec.com/vuln/CYBSEC-Security_Pre-Advisory_SAP_IGS_Remote_Buffer_Overf...
SecurityFocus
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API cve.report/api

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