



CVE-2015-5689

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

Summary

CVE	CVE-2015-5689
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-20 20:59:00 UTC
Updated	2016-12-22 03:00:00 UTC
Description	ghostexp.exe in Ghost Explorer Utility in Symantec Ghost Solutions Suite (GSS) before 3.0 HF2 12.0.0.8010 and Symantec

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Deployment Solution	6.9	sp3	All	All
Application	Symantec	Deployment Solution	6.9	sp3	All	All
Application	Symantec	Ghost Solutions Suite	1.0	All	All	All
Application	Symantec	Ghost Solutions Suite	1.1	All	All	All
Application	Symantec	Ghost Solutions Suite	1.1	p2	All	All
Application	Symantec	Ghost Solutions Suite	2.0	All	All	All
Application	Symantec	Ghost Solutions Suite	2.0.1	All	All	All
Application	Symantec	Ghost Solutions Suite	2.0.2	All	All	All
Application	Symantec	Ghost Solutions Suite	2.1	All	All	All
Application	Symantec	Ghost Solutions Suite	1.0	All	All	All
Application	Symantec	Ghost Solutions Suite	1.1	All	All	All
Application	Symantec	Ghost Solutions Suite	1.1	p2	All	All
Application	Symantec	Ghost Solutions Suite	2.0	All	All	All
Application	Symantec	Ghost Solutions Suite	2.0.1	All	All	All
Application	Symantec	Ghost Solutions Suite	2.0.2	All	All	All
Application	Symantec	Ghost Solutions Suite	2.1	All	All	All

References

Reference

Security Advisories Relating to Symantec Products - Symantec Ghost Explorer Utility Tool Out-of-Bounds Array Indexing - 2015-09-02T05:00:

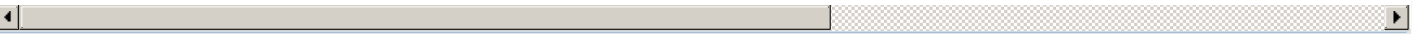
Zero Day Initiative

Symantec Ghost Solutions Suite Array Index Overflow in Processing Files Lets Remote Users Execute Arbitrary Code - SecurityTracker

Symantec Ghost Explorer Utility Out of Bounds Array Indexing Memory Corruption Vulnerability

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](#) 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](#)