



CVE-2015-2994

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

Summary

CVE	CVE-2015-2994
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-08 14:59:00 UTC
Updated	2018-10-09 19:56:00 UTC
Description	Unrestricted file upload vulnerability in ChangePhoto.jsp in SysAid Help Desk before 15.2 allows remote administrators to e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sysaid	Sysaid	All	All	All	All

References

Reference	Source	Link
SysAid Multiple Security Vulnerabilities	BID	www.secu
SysAid 15.2: Your Voice, Your Service Desk	CONFIRM	www.sysai
Full Disclosure: [Multiple CVE's]: various critical vulnerabilities in SysAid Help Desk (RCE, file download, DoS, etc)	FULLDISC	seclists.org
SysAid Help Desk 14.4 Code Execution / Denial Of Service / Traversal / SQL Injection ≈ Packet Storm	MISC	packetstor
SecurityFocus	BUGTRAQ	www.secu
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

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](#)