



CVE-2014-4947

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

Summary

CVE	CVE-2014-4947
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-22 20:55:00 UTC
Updated	2017-08-29 01:35:00 UTC
Description	Buffer overflow in the HVM graphics console support in Citrix XenServer 6.2 Service Pack 1 and earlier has unspecified imp

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Xenserver	6.2.0	sp1	All	All
Application	Citrix	Xenserver	6.2.0	sp1	All	All

References

Reference	Source	Link
Citrix XenServer HVM Graphics CVE-2014-4947 Buffer Overflow Vulnerability	BID	www.se
Citrix XenServer Multiple Security Updates	CONFIRM	support.
Citrix XenServer Flaws Let Local Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTrack	www.se
About Secunia Research Flexera	SECUNIA	secunia
IBM X-Force Exchange	XF	exchang
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

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](#)