



CVE-2012-1508

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2012-1508
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-16 20:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The XPDM display driver in VMware ESXi 4.0, 4.1, and 5.0; VMware ESX 4.0 and 4.1; and VMware View before 4.6.1 allow

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Esx	4.0	All	All	All

Application	Vmware	Esx	4.1	All	All	All
Operating System	Vmware	Esxi	4.0	All	All	All
Operating System	Vmware	Esxi	4.1	All	All	All
Operating System	Vmware	Esxi	5.0	All	All	All
Application	Vmware	View	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References	
Reference	Score
osvdb.org/80115	affected
VMware ESX/ESXi Buffer Overflow and Null Pointer Dereference Lets Local Users Gain Elevated Privileges - SecurityTracker	affected
Security Alerts - Secunia	affected
VMware View Privilege Escalation Vulnerabilities	affected
Repository / Oval Repository	affected
VMSA-2012-0005.3	affected
archives.neohapsis.com/archives/bugtraq/2012-03/0071.html	affected
VMware View Lets Local Users Gain Elevated Privileges and Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	affected
VMSA-2012-0004	affected
Security Advisory SA48379 - VMware View Cross-Site Scripting and Privilege Escalation Vulnerabilities - Secunia	affected
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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