CVE-2015-1758

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

Summary

CVE	CVE-2015-1758
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-10 01:59:30 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Untrusted search path vulnerability in the LoadLibrary function in the kernel in Microsoft Windows Vista SP2, Windows Serv

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 7	All	sp1	x64	All

Operating System	Microsoft	Windows 7	All	sp1	x86	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows Rt	-	All	All	All
Operating System	Microsoft	Windows Server 2008	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All

Vendor Declared Affected Products

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

References

Reference	Source	L
JVN#18146081: LoadLibrary function in Microsoft Windows fails to validate input properly	af854a3a-2127-422b-91ae-364da2661108	j
Microsoft Security Bulletin MS15-063 - Important | Microsoft Docs	af854a3a-2127-422b-91ae-364da2661108	c
Windows Kernel DLL Path Error Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108	v
JVNDB-2015-000086 - JVN iPedia	af854a3a-2127-422b-91ae-364da2661108	j
Microsoft Windows LoadLibrary CVE-2015-1758 Remote Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da2661108	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

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