CVE-2016-0099

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

Summary

CVE	CVE-2016-0099
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-09 11:59:00 UTC
Updated	2018-10-12 22:11:00 UTC
Description	The Secondary Logon Service in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1,

Risk And Classification

EPSS: 0.904310000 probability, percentile 0.996050000 (date 2026-04-07)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Known

Problem Types: CWE-264

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2016-0099

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All

Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	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 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 Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All

References

Reference	Source
Windows - Secondary Logon Standard Handles Missing Sanitization Privilege Escalation MS16-032	EXPLO
Microsoft Windows Secondary Logon CVE-2016-0099 Local Privilege Escalation Vulnerability	BID
Microsoft Windows Secondary Logon Service Handle Processing Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTR
Microsoft Security Bulletin MS16-032 - Important | Microsoft Docs	MS
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Local Privilege Escalation (MS16-032) (C#)	EXPLO
Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Privilege Escalation (MS16-032) (PowerShell)	EXPLO
Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Secondary Logon Handle Privilege Escalation (MS16-032) (Metasploit)	EXPLO
CVE Program record	CVE.OI
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**