



CVE-2014-2848

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

Summary

CVE	CVE-2014-2848
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-11 15:55:22 UTC
Updated	2026-05-06 22:30:45 UTC
Description	A race condition in the wmi_malware_scan.nbin plugin before 201402262215 for Nessus 5.2.1 allows local users to gain pri

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: CWE-362 | 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
Application	Tenable	Nessus	5.2.1	All	All	All

Application	Tenable	Plugin-set	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
Nessus Malicious Process Detection Plugin Lets Local Users Gain Elevated Privileges - SecurityTracker				af854a3a-2127-422b-91a		
Security Advisory SA57403 - Nessus wmi_malware_scan.nbin Plugin Privilege Escalation Vulnerability - Secunia				af854a3a-2127-422b-91a		
Security advisory: Local escalation of privileg... Tenable Discussions Forum				af854a3a-2127-422b-91a		
www.nccgroup.com/en/learning-and-research-centre/technical-advisories/nessus-a...				af854a3a-2127-422b-91a		
CVE Program record				CVE.ORG		
NVD vulnerability detail				NVD		
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](#)