



# platform/x86: dell-wmi-sysman: Don't hex dump plaintext password data

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

## Summary

<b>CVE</b>	CVE-2026-23370
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 11:16:36 UTC
<b>Updated</b>	2026-04-18 09:16:21 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: platform/x86: dell-wmi-sysman: Don't hex dump plaintext p

## Risk And Classification

**EPSS:** 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d 9bbb420f202834363e1e25435e49db0a385c2232 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d d9e785bd62d2ac23cf29a75dcfea8c8087fd3870 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d 411ba3cd837f7825c0e648e155bc505641f95854 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d 0e6115c2f2facaed9593c16ad2e5accd487f5c52 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d 5de34126fb2edf8ab7f25d677b132e92d8bf9ede git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d d78e74adc5cff7afd9d03b9da8058a7e435f9bc git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected e8a60aa7404bfef37705da5607c97737073ac38d d1a196e0a6dcddd03748468a0e9e3100790fc85c gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.11
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.11 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.167 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.130 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.77 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.17 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.7 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original commit for fix

References				
Reference	Source	Link	Tags	
<a href="https://git.kernel.org/stable/c/d1a196e0a6dcddd03748468a0e9e3100790fc85c">git.kernel.org/stable/c/d1a196e0a6dcddd03748468a0e9e3100790fc85c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/411ba3cd837f7825c0e648e155bc505641f95854">git.kernel.org/stable/c/411ba3cd837f7825c0e648e155bc505641f95854</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/9bbb420f202834363e1e25435e49db0a385c2232">git.kernel.org/stable/c/9bbb420f202834363e1e25435e49db0a385c2232</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/0e6115c2f2facaed9593c16ad2e5accd487f5c52">git.kernel.org/stable/c/0e6115c2f2facaed9593c16ad2e5accd487f5c52</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/d9e785bd62d2ac23cf29a75dcfea8c8087fd3870">git.kernel.org/stable/c/d9e785bd62d2ac23cf29a75dcfea8c8087fd3870</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/d78e74adc5cff7afd9d03b9da8058a7e435f9bc">git.kernel.org/stable/c/d78e74adc5cff7afd9d03b9da8058a7e435f9bc</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
<a href="https://git.kernel.org/stable/c/5de34126fb2edf8ab7f25d677b132e92d8bf9ede">git.kernel.org/stable/c/5de34126fb2edf8ab7f25d677b132e92d8bf9ede</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>		
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic	

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)