



# x86/efi: defer freeing of boot services memory

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

## Summary

<b>CVE</b>	CVE-2026-23352
<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 11:16:33 UTC
<b>Updated</b>	2026-04-18 09:16:20 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: x86/efi: defer freeing of boot services memory efi_free_bo

## Risk And Classification

**EPSS:** 0.000430000 probability, percentile 0.131160000 (date 2026-04-18)

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0aed459e8487eb6ebdb4efe8cfe1eafbc704b30 4a2cb90c538f06c873a187aa743575d48685d7a6 git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 7131bd1fecc749bc94fb44aae217bbd8a8a85264 git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 6d8ba221e7aafaa2f284b7d22faee814c28e009d git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 227688312fece0026fc67a00ba9a0b3611e9e95d git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 6a25e25279282c5c8ade554c04c6ab9dc7902c64 git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 399da820ecfe6f4f10c143e5c453d3559a04db9c git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 f9e9cc320854a76a39e7bc92d144554f3a727fad git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 7dcf59422a3b0d20ddda844f856b4a1e0608a326 git
CNA	Linux	Linux	affected 916f676f8dc016103f983c7ec54c18ecd6bb6e349 a4b0bf6a40f3c107c67a24fbc614510ef5719980 git
CNA	Linux	Linux	affected 3.0
CNA	Linux	Linux	unaffected 3.0 semver
CNA	Linux	Linux	unaffected 2.6.39.2 2.6.* semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	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/a4b0bf6a40f3c107c67a24fbc614510ef5719980">git.kernel.org/stable/c/a4b0bf6a40f3c107c67a24fbc614510ef5719980</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/4a2cb90c538f06c873a187aa743575d48685d7a6">git.kernel.org/stable/c/4a2cb90c538f06c873a187aa743575d48685d7a6</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f9e9cc320854a76a39e7bc92d144554f3a727fad">git.kernel.org/stable/c/f9e9cc320854a76a39e7bc92d144554f3a727fad</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/399da820ecfe6f4f10c143e5c453d3559a04db9c">git.kernel.org/stable/c/399da820ecfe6f4f10c143e5c453d3559a04db9c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6d8ba221e7aafaa2f284b7d22faee814c28e009d">git.kernel.org/stable/c/6d8ba221e7aafaa2f284b7d22faee814c28e009d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/227688312fece0026fc67a00ba9a0b3611ebe95d">git.kernel.org/stable/c/227688312fece0026fc67a00ba9a0b3611ebe95d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7131bd1fecc749bc94fb44aae217bbd8a8a85264">git.kernel.org/stable/c/7131bd1fecc749bc94fb44aae217bbd8a8a85264</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7dcf59422a3b0d20ddda844f856b4a1e0608a326">git.kernel.org/stable/c/7dcf59422a3b0d20ddda844f856b4a1e0608a326</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/6a25e25279282c5c8ade554c04c6ab9dc7902c64">git.kernel.org/stable/c/6a25e25279282c5c8ade554c04c6ab9dc7902c64</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](#) 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](https://cve.report/api)

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