



# CVE-2022-29264

Published on: Not Yet Published

Last Modified on: 09/30/2022 01:06:00 PM UTC

## CVE-2022-29264

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Coreboot](#) from [Coreboot](#) contain the following vulnerability:

An issue was discovered in coreboot 4.13 through 4.16. On APs, arbitrary code execution in SMM may occur.

CVE-2022-29264 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                             | Tags                                                    | Link                                                                                                                 |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| cpu/x86/smm: Introduce SMM module loader version 2 · coreboot/coreboot@afb7a81 · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">github.com/coreboot/coreboot/commit/afb7a814783cda12f5b72167163b9109ee1d15a7</a> |

No Description Provided

[review.coreboot.org](https://review.coreboot.org)  
[text/html](#)

 [MISC review.coreboot.org/c/coreboot/+/#63478](https://review.coreboot.org/c/coreboot/+/#63478)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type                               | Vendor                   | Product                  | Version | Update | Edition | Language |
|------------------------------------|--------------------------|--------------------------|---------|--------|---------|----------|
| Application                        | <a href="#">Coreboot</a> | <a href="#">Coreboot</a> | All     | All    | All     | All      |
| Operating System                   | <a href="#">Coreboot</a> | <a href="#">Coreboot</a> | All     | All    | All     | All      |
| cpe:2.3:a:coreboot:coreboot:*****: |                          |                          |         |        |         |          |
| cpe:2.3:o:coreboot:coreboot:*****: |                          |                          |         |        |         |          |

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                                                                                            | Title                                                                                                                                                                                                    | Posted (UTC)        |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport     | CVE-2022-29264 : An issue was discovered in coreboot 4.13 through 4.16. On APs, arbitrary code execution in SMM may... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-04-25 07:06:56 |
|  @Robo_Alerts   | Potentially Critical CVE Detected! CVE-2022-29264 An issue was discovered in coreboot 4.13 through 4.16. On APs, ar... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-04-25 07:56:01 |
|  @threatmeter   | CVE-2022-29264 An issue was discovered in coreboot 4.13 through 4.16. On APs, arbitrary code execution in SMM may o... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-04-25 23:04:41 |
|  @hardenedvault | CVE-2022-29264: SMM can be hijacked by the OS on APs #coreboot #firmware                                                                                                                                 | 2022-04-26 06:06:07 |
|  /r/netcve      | <a href="#">CVE-2022-29264</a>                                                                                                                                                                           | 2022-04-25 07:39:12 |

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)