

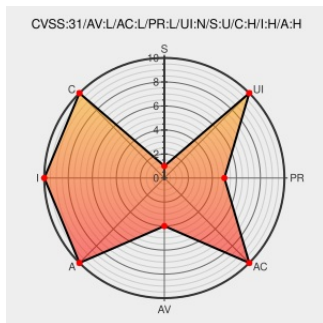


CVE-2023-22297

Published on: Not Yet Published

Last Modified on: 05/18/2023 07:11:00 PM UTC

CVE-2023-22297

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

Certain versions of [Server System D50tnp1mhcpac](#) from [Intel](#) contain the following vulnerability:

Access of memory location after end of buffer in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access.

CVE-2023-22297 has been assigned by [intel](#) secure@intel.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
INTEL-SA-00839	www.intel.com text/html	intel MISC www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00839.html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Hardware 	Intel	Server System D50tnp1mhcpac	-	All	All	All
Operating System	Intel	Server System D50tnp1mhcpac Firmware	All	All	All	All
Hardware 	Intel	Server System D50tnp1mhcrac	-	All	All	All
Operating System	Intel	Server System D50tnp1mhcrac Firmware	All	All	All	All
Hardware 	Intel	Server System D50tnp1mhcrlc	-	All	All	All
Operating System	Intel	Server System D50tnp1mhcrlc Firmware	All	All	All	All
Hardware 	Intel	Server System D50tnp2mfalac	-	All	All	All
Operating System	Intel	Server System D50tnp2mfalac Firmware	All	All	All	All
Hardware 	Intel	Server System D50tnp2mhstac	-	All	All	All
Operating System	Intel	Server System D50tnp2mhstac Firmware	All	All	All	All
Hardware 	Intel	Server System D50tnp2mhsvac	-	All	All	All
Operating System	Intel	Server System D50tnp2mhsvac Firmware	All	All	All	All
Hardware 	Intel	Server System M50cyp1ur204	-	All	All	All
Operating System	Intel	Server System M50cyp1ur204 Firmware	All	All	All	All
Hardware 	Intel	Server System M50cyp1ur212	-	All	All	All
Operating System	Intel	Server System M50cyp1ur212 Firmware	All	All	All	All
Hardware 	Intel	Server System M50cyp2ur208	-	All	All	All
Operating System	Intel	Server System M50cyp2ur208 Firmware	All	All	All	All
Hardware 	Intel	Server System M50cyp2ur312	-	All	All	All
Operating System	Intel	Server System M50cyp2ur312 Firmware	All	All	All	All
cpe:2.3:h:intel:server_system_d50tnp1mhcpac:-:*****:						
cpe:2.3:o:intel:server_system_d50tnp1mhcpac_firmware:*****:						
cpe:2.3:h:intel:server_system_d50tnp1mhcrac:-:*****:						
cpe:2.3:o:intel:server_system_d50tnp1mhcrac_firmware:*****:						
cpe:2.3:h:intel:server_system_d50tnp1mhcrlc:-:*****:						
cpe:2.3:o:intel:server_system_d50tnp1mhcrlc_firmware:*****:						
cpe:2.3:h:intel:server_system_d50tnp2mfalac:*****:						

cpe:2.3:o:intel:server_system_d50tnp2mfalac_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_d50tnp2mhstac:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_d50tnp2mhstac_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_d50tnp2mhsvac:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_d50tnp2mhsvac_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_m50cyp1ur204:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_m50cyp1ur204_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_m50cyp1ur212:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_m50cyp1ur212_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_m50cyp2ur208:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_m50cyp2ur208_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:intel:server_system_m50cyp2ur312:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:intel:server_system_m50cyp2ur312_firmware:*.*.*.*.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒@CVEreport	CVE-2023-22297 : Access of memory location after end of buffer in some Intel R Server Board BMC firmware before ve... twitter.com/i/web/status/1...	2023-05-10 14:27:06

[← 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