



# CVE-2020-12299

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

## Summary

<b>CVE</b>	CVE-2020-12299
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@intel.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-13 04:15:00 UTC
<b>Updated</b>	2020-08-19 17:55:00 UTC
<b>Description</b>	Improper input validation in BIOS firmware for Intel(R) Server Board Families S2600ST, S2600BP and S2600WF may allow

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Intel	S2600bpbr	-	All	All	All
Hardware	Intel	S2600bpbr	-	All	All	All
Operating System	Intel	S2600bpbr Firmware	All	All	All	All
Operating System	Intel	S2600bpbr Firmware	All	All	All	All
Hardware	Intel	S2600bpqr	-	All	All	All
Hardware	Intel	S2600bpqr	-	All	All	All
Operating System	Intel	S2600bpqr Firmware	All	All	All	All
Operating System	Intel	S2600bpqr Firmware	All	All	All	All
Hardware	Intel	S2600bpsr	-	All	All	All
Hardware	Intel	S2600bpsr	-	All	All	All
Operating System	Intel	S2600bpsr Firmware	All	All	All	All
Operating System	Intel	S2600bpsr Firmware	All	All	All	All
Hardware	Intel	S2600stbr	-	All	All	All
Hardware	Intel	S2600stbr	-	All	All	All
Operating System	Intel	S2600stbr Firmware	All	All	All	All
Operating System	Intel	S2600stbr Firmware	All	All	All	All
Hardware	Intel	S2600stqr	-	All	All	All

Hardware	<a href="#">Intel</a>	<a href="#">S2600stqr</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600stqr Firmware</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600stqr Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wf0r</a>	-	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wf0r</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wf0r Firmware</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wf0r Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wfqr</a>	-	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wfqr</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wfqr Firmware</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wfqr Firmware</a>	All	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wftr</a>	-	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">S2600wftr</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wftr Firmware</a>	All	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">S2600wftr Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Ta
Intel-SA-00367	MISC	<a href="http://www.intel.com">www.intel.com</a>	Pa
Intel SA-00367 Server Board Firmware Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	Th
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	ca

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](#).

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