



CVE-2020-29022

Published on: 02/16/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

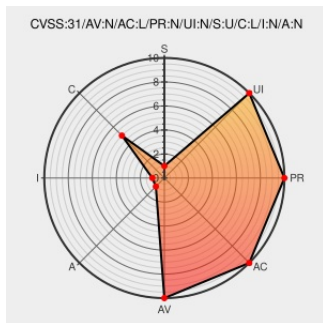
CVE-2020-29022

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Gatemanager 4250](#) from [Secomea](#) contain the following vulnerability:

Failure to Sanitize host header value on output in the GateManager Web server could allow an attacker to conduct web cache poisoning attacks. This issue affects Secomea GateManager all versions prior to 9.3

CVE-2020-29022 has been assigned by VulnerabilityReporting@secomea.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Secomea** - **GateManager** version < 9.3

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Cybersecurity Advisory - Secomea	Vendor Advisory www.secomea.com	MISC www.secomea.com/support/cybersecurity-advisory/#2923

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  	Secomea	Gatemanager 4250	-	All	All	All
Hardware  	Secomea	Gatemanager 4250	-	All	All	All
Operating System	Secomea	Gatemanager 4250 Firmware	All	All	All	All
Operating System	Secomea	Gatemanager 4250 Firmware	All	All	All	All
Hardware  	Secomea	Gatemanager 4260	-	All	All	All
Hardware  	Secomea	Gatemanager 4260	-	All	All	All
Operating System	Secomea	Gatemanager 4260 Firmware	All	All	All	All
Operating System	Secomea	Gatemanager 4260 Firmware	All	All	All	All
Hardware  	Secomea	Gatemanager 8250	-	All	All	All
Hardware  	Secomea	Gatemanager 8250	-	All	All	All
Operating System	Secomea	Gatemanager 8250 Firmware	All	All	All	All
Operating System	Secomea	Gatemanager 8250 Firmware	All	All	All	All
Hardware  	Secomea	Gatemanager 9250	-	All	All	All
Hardware  	Secomea	Gatemanager 9250	-	All	All	All
Operating System	Secomea	Gatemanager 9250 Firmware	All	All	All	All
Operating System	Secomea	Gatemanager 9250 Firmware	All	All	All	All

```
cpe:2.3:h:secomea:gatemanager_4250:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:secomea:gatemanager_4250:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:secomea:gatmanager_4250_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:secomea:gatmanager_4250_firmware:*.*.*.*.*.*.*
```

cpe:2.3:h:secomea:gatemanager_4260:-:*:*:*:*:*:
cpe:2.3:h:secomea:gatemanager_4260:-:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_4260_firmware:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_4260_firmware:*:*:*:*:*:
cpe:2.3:h:secomea:gatemanager_8250:-:*:*:*:*:*:
cpe:2.3:h:secomea:gatemanager_8250:-:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_8250_firmware:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_8250_firmware:*:*:*:*:*:
cpe:2.3:h:secomea:gatemanager_9250:-:*:*:*:*:*:
cpe:2.3:h:secomea:gatemanager_9250:-:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_9250_firmware:*:*:*:*:*:
cpe:2.3:o:secomea:gatemanager_9250_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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