



CVE-2019-10940

Published on: 01/16/2020 12:00:00 AM UTC

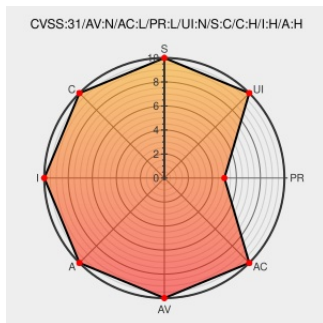
Last Modified on: 09/20/2021 12:15:00 PM UTC

CVE-2019-10940

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Sinema Server](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SINEMA Server (All versions < V14.0 SP2 Update 1). Incorrect session validation could allow an attacker with a valid session, with low privileges, to perform firmware updates and other administrative operations on connected devices.

The security vulnerability could be exploited by an attacker with network access to the affected system. An attacker must have access to a low privileged account in order to exploit the vulnerability. An attacker could use the vulnerability to compromise confidentiality, integrity, and availability of the affected system and underlying components. At the time of advisory publication no public exploitation of this security vulnerability was known.

CVE-2019-10940 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [S](#) **Siemens AG - SINEMA Server** version **All versions < V14.0 SP2 Update 1**



CVSS3 Score: **9.9 - CRITICAL**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
	Vendor Advisory cert-portal.siemens.com application/pdf	 CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-880233.pdf
Siemens SINEMA Server CISA	Third Party Advisory www.us-cert.gov text/html	 MISC www.us-cert.gov/ics/advisories/icsa-20-014-02

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	Siemens	Sinema Server	-	All	All	All
Hardware	Siemens	Sinema Server	-	All	All	All
Application	Siemens	Sinema Server	All	All	All	All
Application	Siemens	Sinema Server	14.0	-	All	All
Application	Siemens	Sinema Server	14.0	sp1	All	All
Application	Siemens	Sinema Server	14.0	sp2	All	All
Operating System	Siemens	Sinema Server Firmware	All	All	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	-	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	sp1	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	sp2	All	All
Operating System	Siemens	Sinema Server Firmware	All	All	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	-	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	sp1	All	All
Operating System	Siemens	Sinema Server Firmware	14.0	sp2	All	All

```
cpe:2.3:h:siemens:sinema_server:-:*:*:*:*:*:
```

```
2.3:h:siemens:sinema_server:-:*:*:*:*:*:
```

cpe:2.3:n:siemens:sinema_server:-:~::~:~::~:
cpe:2.3:a:siemens:sinema_server:~::~:~::~:~::~:
cpe:2.3:a:siemens:sinema_server:14.0:-:~::~:~::~:~::~:
cpe:2.3:a:siemens:sinema_server:14.0:sp1:~::~:~::~:~::~:
cpe:2.3:a:siemens:sinema_server:14.0:sp2:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:-:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:sp1:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:sp2:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:-:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:sp1:~::~:~::~:~::~:
cpe:2.3:o:siemens:sinema_server_firmware:14.0:sp2:~::~:~::~:~::~:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 [T](#) [N](#) |

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](#)