



CVE-2020-7584

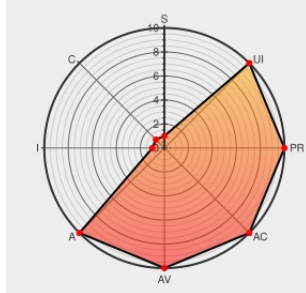
Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7584

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

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



Certain versions of [Simatic S7-200 Smart Sr Cpu](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SIMATIC S7-200 SMART CPU family (All versions $\geq$ V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incoming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation.

CVE-2020-7584 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens AG - SIMATIC S7-200 SMART CPU family** version **All versions $\geq$ V2.2 < V2.5.1**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
	Vendor Advisory	MISC cert-portal.siemens.com/productcert/pdf/ssa-589181.pdf

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Simatic S7-200 Smart Sr Cpu	-	All	All	All
Hardware	Siemens	Simatic S7-200 Smart Sr Cpu	-	All	All	All
Operating System	Siemens	Simatic S7-200 Smart Sr Cpu Firmware	All	All	All	All
Operating System	Siemens	Simatic S7-200 Smart Sr Cpu Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-200 Smart St Cpu	-	All	All	All
Hardware	Siemens	Simatic S7-200 Smart St Cpu	-	All	All	All
Operating System	Siemens	Simatic S7-200 Smart St Cpu Firmware	All	All	All	All
Operating System	Siemens	Simatic S7-200 Smart St Cpu Firmware	All	All	All	All
cpe:2.3:h:siemens:simatic_s7-200_smart_sr_cpu:-:~::~:						
cpe:2.3:h:siemens:simatic_s7-200_smart_sr_cpu:-:~::~:						
cpe:2.3:o:siemens:simatic_s7-200_smart_sr_cpu_firmware:*~::~:						
cpe:2.3:o:siemens:simatic_s7-200_smart_sr_cpu_firmware:*~::~:						
cpe:2.3:h:siemens:simatic_s7-200_smart_st_cpu:-:~::~:						
cpe:2.3:h:siemens:simatic_s7-200_smart_st_cpu:-:~::~:						
cpe:2.3:o:siemens:simatic_s7-200_smart_st_cpu_firmware:*~::~:						
cpe:2.3:o:siemens:simatic_s7-200_smart_st_cpu_firmware:*~::~:						

Next ID→

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](#)