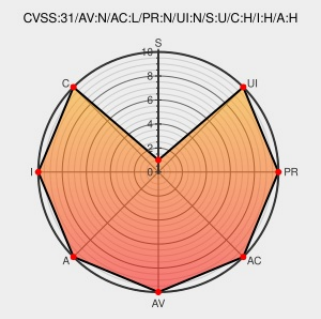
CVE-2021-40358

Published on: 11/09/2021 12:00:00 AM UTC

Last Modified on: 10/19/2022 07:36:00 PM UTC

CVE-2021-40358

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Simatic Pcs 7 from Siemens contain the following vulnerability:

A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3 UC04), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 5). Legitimate file operations on the web server of the affected systems do not properly neutralize special elements within the pathname. An attacker could then cause the pathname to resolve to a location outside of the restricted directory on the server and read, write or delete unexpected critical files.

CVE-2021-40358 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-840188.pdf

Related QID Numbers

590822 Siemens SIMATIC WinCC (Update B) Multiple Vulnerabilities (ICSA-21-315-03)

Exploit/POC from Github

A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP3…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Pcs 7	All	All	All	All
Application	Siemens	Simatic Pcs 7	8.2	All	All	All
Application	Siemens	Simatic Pcs 7	9.0	-	All	All
Application	Siemens	Simatic Pcs 7	9.1	All	All	All
Application	Siemens	Simatic Pcs 7	9.1	-	All	All
Application	Siemens	Simatic Pcs 7	All	All	All	All
Application	Siemens	Simatic Wincc	All	All	All	All
Application	Siemens	Simatic Wincc	15	All	All	All
Application	Siemens	Simatic Wincc	15.1	-	All	All
Application	Siemens	Simatic Wincc	15.1	update_1	All	All
Application	Siemens	Simatic Wincc	15.1	update_2	All	All
Application	Siemens	Simatic Wincc	15.1	update_3	All	All
Application	Siemens	Simatic Wincc	15.1	update_4	All	All
Application	Siemens	Simatic Wincc	15.1	update_5	All	All
Application	Siemens	Simatic Wincc	15.1	update_6	All	All
Application	Siemens	Simatic Wincc	16	All	All	All
Application	Siemens	Simatic Wincc	16	update1	All	All
Application	Siemens	Simatic Wincc	16	update2	All	All
Application	Siemens	Simatic Wincc	16	update3	All	All

Application	Siemens	Simatic Wincc	16	update4	All	All
Application	Siemens	Simatic Wincc	17	All	All	All
Application	Siemens	Simatic Wincc	17	update1	All	All
Application	Siemens	Simatic Wincc	7.4	All	All	All
Application	Siemens	Simatic Wincc	7.4	-	All	All
Application	Siemens	Simatic Wincc	7.4	sp1	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update1	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update10	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update11	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update12	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update13	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update14	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update15	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update16	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update17	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update18	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update2	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update3	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update4	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update5	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update6	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update7	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update8	All	All
Application	Siemens	Simatic Wincc	7.4	sp1_update9	All	All
Application	Siemens	Simatic Wincc	7.4	update_1	All	All
Application	Siemens	Simatic Wincc	7.5	All	All	All
Application	Siemens	Simatic Wincc	7.5	-	All	All
Application	Siemens	Simatic Wincc	7.5	sp1	All	All
Application	Siemens	Simatic Wincc	7.5	sp1_update1	All	All
Application	Siemens	Simatic Wincc	7.5	sp1_update2	All	All
Application	Siemens	Simatic Wincc	7.5	sp2	All	All
Application	Siemens	Simatic Wincc	7.5	sp2_update1	All	All
Application	Siemens	Simatic Wincc	7.5	sp2_update2	All	All
Application	Siemens	Simatic Wincc	7.5	sp2_update3	All	All
Application	Siemens	Simatic Wincc	7.5	sp2_update4	All	All
Application	Siemens	Simatic Wincc	All	All	All	All

Application	Siemens	Simatic Wincc	All	All	All	All

cpe:2.3:a:siemens:simatic_pcs_7:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs_7:8.2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs_7:9.0:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs_7:9.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs_7:9.1:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_pcs_7:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_1:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_2:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_3:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_4:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_5:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:15.1:update_6:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:16:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:16:update1:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:16:update2:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:16:update3:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:16:update4:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:17:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:17:update1:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update1:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update10:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update11:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update12:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update13:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update14:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update15:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update16:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update17:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update18:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update3:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update5:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update6:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update7:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update8:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:sp1_update9:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:update_1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp1_update1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp1_update2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp2_update1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp2_update2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp2_update3:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.5:sp2_update4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40358 : A vulnerability has been identified in SIMATIC PCS 7 V8.2 and earlier All versions , SIMATIC PCS… twitter.com/i/web/status/1…	2021-11-09 11:47:16

← Previous ID

Next ID→