

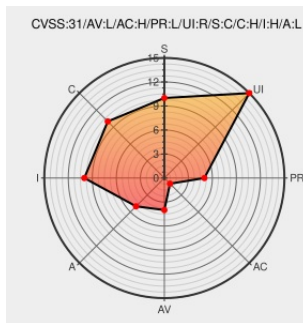


CVE-2020-7360

Published on: 08/13/2020 12:00:00 AM UTC

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

CVE-2020-7360

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

Certain versions of [Smartcontrol](#) from [Philips](#) contain the following vulnerability:

An Uncontrolled Search Path Element (CWE-427) vulnerability in SmartControl version 4.3.15 and versions released before April 15, 2020 may allow an authenticated user to escalate privileges by placing a specially crafted DLL file in the search path. This issue was fixed in version 1.0.7, which was released after April 15, 2020. (Note, the version numbering system changed significantly between version 4.3.15 and version 1.0.7.)

CVE-2020-7360 has been assigned by [cve@rapid7.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Philips](#) - **SmartControl** version = **4.3.15**

Affected Vendor/Software: [Philips](#) - **SmartControl** version ! **1.0.7**

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

Philips SmartControl DLL hijacking (CVE-2020-7360)

Tags

Exploit

Third Party Advisory

blog.vonahi.io

text/html

Link

MISC

blog.vonahi.io/when-the-path-to-system-is-wide-open/

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
Application	Philips	Smartcontrol	All	All	All	All
cpe:2.3:a:philips:smartcontrol:*****:						

Discovery Credit

This issue was discovered and reported by Erik Wynter of Vonahi Security.

← Previous ID

Next ID →