

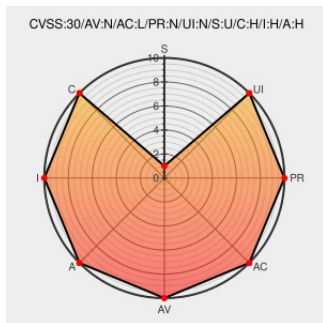


CVE-2017-10832

Published on: 08/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-10832

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

Certain versions of [Scr02hd](#) from [Nippon-antenna](#) contain the following vulnerability:

"Dokodemo eye Smart HD" SCR02HD Firmware 1.0.3.1000 and earlier allows remote attackers to execute arbitrary OS commands via unspecified vectors.

CVE-2017-10832 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [NIPPON ANTENNA Co., Ltd](#) - "Dokodemo eye Smart HD" SCR02HD version **Firmware 1.0.3.1000 and earlier**

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: **10 - HIGH**

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

CVE References

Description	Tags	Link
JVN#87410770: Multiple vulnerabilities in "Dokodemo eye Smart HD" SCR02HD	Third Party Advisory VDB Entry	JVN JVN#87410770

Vendor Advisory
www.nippon-antenna.co.jp
application/pdf
Inactive Link Not Archived

▲ MISC www.nippon-antenna.co.jp/product/ine/pdf/scr02hd_about_security.pdf

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  	Nippon-antenna	Scr02hd	-	All	All	All
Hardware  	Nippon-antenna	Scr02hd	-	All	All	All
Operating System	Nippon-antenna	Scr02hd Firmware	All	All	All	All
cpe:2.3:h:nippon-antenna:scr02hd:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:nippon-antenna:scr02hd:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:nippon-antenna:scr02hd_firmware:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

Next ID→