



CVE-2020-6785

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6785
State	PUBLIC
Assigner	psirt@bosch.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-25 16:15:00 UTC
Updated	2021-03-25 18:16:00 UTC
Description	Loading a DLL through an Uncontrolled Search Path Element in Bosch BVMS and BVMS Viewer in versions 10.1.0, 10.0.1

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Bosch	Divar Ip 7000 R2	-	All	All	All
Hardware	Bosch	Divar Ip All-in-one 5000	-	All	All	All
Hardware	Bosch	Divar Ip All-in-one 7000	-	All	All	All
Application	Bosch	Video Management System	All	All	All	All
Application	Bosch	Video Management System Viewer	All	All	All	All

References

Reference	Source	Link	Tags
Uncontrolled Search Path Element in Multiple Bosch Products Bosch PSIRT	CONFIRM	psirt.bosch.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)