

BVMS affected by Autodesk Design Review Multiple Vulnerabilities

BOSCH-SA-246962-BT

Advisory Information

Advisory ID: BOSCH-SA-246962-BT

CVE Numbers and CVSS v3.1 Scores:

[CVE-2021-27033](#)

Base Score: 7.8 (High)

[CVE-2021-27034](#)

Base Score: 7.8 (High)

[CVE-2021-27035](#)

Base Score: 7.8 (High)

[CVE-2021-27036](#)

Base Score: 7.8 (High)

[CVE-2021-27037](#)

Base Score: 7.8 (High)

[CVE-2021-27038](#)

Base Score: 7.8 (High)

[CVE-2021-27039](#)

Base Score: 7.8 (High)

Published: 13 Mar 2024

Last Updated: 13 Mar 2024

Summary

BVMS was using Autodesk Design Review for showing 2D/3D files. Autodesk has published multiple vulnerabilities which when successfully exploited could lead to the

execution of arbitrary code.

Starting from BVMS version 11.0, the Autodesk Design Review is not used anymore in BVMS, but the BVMS setup does not uninstall the Autodesk Design Review during a BVMS upgrade. This means only BVMS systems are affected which have versions $\leq$ 10.1.1.12 or were upgraded from BVMS Version $\leq$ 10.1.1.12 to a higher version.

Bosch does not provide any patches for BVMS $\leq$ 10.1.1.12

For BVMS systems upgraded from any BVMS version $\leq$ 10.1.1.12 Bosch advises to mitigate the vulnerability.

Fresh BVMS installations starting from BVMS 11.0 are not affected

Before removing Autodesk Design Review v 9.1.0.127 make sure that it is not used by any other software installed on that machine.

How to check if the system is affected:

In the Search bar, search for "add remove" and select "Add remove programs".

Check whether Autodesk Design Review v 9.1.0.127 is installed.

Affected Products

Bosch BVMS

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.1 (including)

Bosch BVMS Viewer

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.1 (including)

Bosch DIVAR IP 7000 R2

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.0.1 (including)

Bosch DIVAR IP all-in-one 5000

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.1 (including)

Bosch DIVAR IP all-in-one 7000

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.1 (including)

Bosch DIVAR IP all-in-one 7000 R3

CVE-2021-27033, CVE-2021-27034, CVE-2021-27035, CVE-2021-27036,
CVE-2021-27037, CVE-2021-27038, CVE-2021-27039

Version(s): 11.0 - 12.1 (including)

Solution and Mitigations

Software Updates

No software updates available. Please refer to the solution on section 4.2 "Uninstall Autodesk Design Review"

Uninstall Autodesk Design Review

Install patch

BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRemovalBeforeUninstall.zip. This step must be executed as the first one and is mandatory.

In the Search bar, search for "add remove" and select "Add remove programs".

Uninstall Autodesk Design Review.

Vulnerability Details

CVE-2021-27033

CVE description: A Double Free vulnerability allows remote attackers to execute

arbitrary code on PDF files within affected installations of Autodesk Design Review 2018, 2017, 2013, 2012, 2011. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

Problem Type:

[CWE-415](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27034

CVE description: A heap-based buffer overflow could occur while parsing PICT, PCX, RCL or TIFF files in Autodesk Design Review 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.

Problem Type:

[CWE-787](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27035

CVE description: A maliciously crafted TIFF, TIF, PICT, TGA, or DWF files in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PICT, TGA or DWF files. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.

Problem Type:

[CWE-787](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27036

CVE description: A maliciously crafted PCX, PICT, RCL, TIF, BMP, PSD or TIFF file can be used to write beyond the allocated buffer while parsing PCX, PDF, PICT, RCL, BMP, PSD or TIFF files. This vulnerability can be exploited to execute arbitrary code

Problem Type:

[CWE-787](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27037

CVE description: A maliciously crafted PNG, PDF or DWF file in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability may be exploited by remote malicious actors to execute arbitrary code.

Problem Type:

[CWE-416](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27038

CVE description: A Type Confusion vulnerability in Autodesk Design Review 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. A malicious actor can leverage this to execute arbitrary code.

Problem Type:

[CWE-843](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

CVE-2021-27039

CVE description: A maliciously crafted TIFF and PCX file can be forced to read and write beyond allocated boundaries when parsing the TIFF and PCX file for based overflow. This vulnerability can be exploited to execute arbitrary code.

Problem Type:

[CWE-787](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Base Score: 7.8 (High)

Remarks

Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.

CVSS Scoring

Vulnerability classification has been performed using the [CVSS v3.1 scoring system](#) . The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

Additional Resources

- [1] BVMS Download Area: <https://downloadstore.boschsecurity.com/index.php?type=BVMS>
- [2] BVMS Viewer Download Area: <https://downloadstore.boschsecurity.com/index.php?type=BVMSVWR>
- [3] BVMS Appliances (DIVAR IP) Download Area: <https://downloadstore.boschsecurity.com/?type=DIPBVMS>

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com .

Revision History

Appendix

Fixes for the Affected Products

BVMS

Affected versions	Version or patch that fixes the vulnerability
Upgraded from <= 10.1.1.12	BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRemovalBe

[BVMS Download Area](#)

BVMS Viewer

Affected versions	Version or patch that fixes the vulnerability
Upgraded from <= 10.1.1.12	BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRemovalBe

[BVMS Viewer Download Area](#)

Bosch DIVAR IP all-in-one 7000 R3

Affected BVMS versions

Version or patch that fixes the vulnerability

Upgraded from <= 10.1.1.12

BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRen

[BVMS Download Area](#)

Bosch DIVAR IP 7000 R2

Affected BVMS versions

Version or patch that fixes the vulnerability

Upgraded from <= 10.1.1.12

BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRen

[BVMS Download Area](#)

Bosch DIVAR IP all-in-one 5000

Affected BVMS versions

Version or patch that fixes the vulnerability

Upgraded from <= 10.1.1.12

BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRen

[BVMS Download Area](#)

Bosch DIVAR IP all-in-one 7000

Affected BVMS versions**Version or patch that fixes the vulnerability**

Upgraded from <= 10.1.1.12

BVMS_AutodeskDesignReview2009_Patch_FixRegKeyRen

[BVMS Download Area](#)

Material Lists

BVMS

Family Name	Versions	CTN	SAP#	Material description
BVMS Professional	11.1.1, 12.0, 12.0.1, 12.1	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus	11.1.1, 12.0, 12.0.1, 12.1	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Plus DIP	11.1.1, 12.0, 12.0.1, 12.1	MBV-BPLU-DIP	F.01U.374.503	License Plus base for DIVAR IP
BVMS Lite	11.1.1,	MBV-	F.01U.393.648	License Lite base

Family Name	Versions	CTN	SAP#	Material descriptio
	12.0, 12.0.1, 12.1	BLIT		
BVMS Lite DIP	11.1.1, 12.0, 12.0.1, 12.1	MBV- BLIT- DIP	F.01U.358.975	License Lite base f DIVAR IP
BVMS Viewer	11.1.1, 12.0, 12.0.1, 12.1	MBV- BVWR	F.01U.393.649	License Viewer bas

Bosch DIVAR IP 7000 R2

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7180-00N	F.01U.314.520	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000 R2	DIP-7183-4HD	F.01U.314.521	DIVAR IP 7000 2U 4x3TB
DIVAR IP 7000 R2	DIP-7183-8HD	F.01U.314.522	DIVAR IP 7000 2U 8x3TB

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7184-4HD	F.01U.314.523	DIVAR IP 7000 2U 4x4TB
DIVAR IP 7000 R2	DIP-7184-8HD	F.01U.314.524	DIVAR IP 7000 2U 8x4TB
DIVAR IP 7000 R2	DIP-71F0-00N	F.01U.314.525	DIVAR IP 7000 3U w/o HDD
DIVAR IP 7000 R2	DIP-71F3-16HD	F.01U.314.526	DIVAR IP 7000 3U 16x3TB
DIVAR IP 7000 R2	DIP-71F4-16HD	F.01U.314.527	DIVAR IP 7000 3U 16x4TB
DIVAR IP 7000 R2	DIP-7186-8HD	F.01U.329.143	DIVAR IP 7000 2U 8x6TB
DIVAR IP 7000 R2	DIP-7188-8HD	F.01U.329.144	DIVAR IP 7000 2U 8x8TB
DIVAR IP 7000 R2	DIP-71F6-16HD	F.01U.329.145	DIVAR IP 7000 3U 16x6TB
DIVAR IP 7000 R2	DIP-71F8-16HD	F.01U.329.146	DIVAR IP 7000 3U 16x8TB
DIVAR IP 7000 R2	DIP-7184-8HD- WAG	F.01U.343.277	DIVAR IP 7000 2U 8x4TB, WAG Kit

Bosch DIVAR IP all-in-one 5000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-5240IG-00N	F.01U.361.821	Management Appliance w/o HDD
DIVAR IP all-in-one 5000	DIP-5244IG-4HD	F.01U.362.424	Management Appliance 4x4TB
DIVAR IP all-in-one 5000	DIP-5248IG-4HD	F.01U.362.423	Management Appliance 4x8TB
DIVAR IP all-in-one 5000	DIP-524CIG-4HD	F.01U.362.422	Management Appliance 4x12TB
DIVAR IP all-in-one 5000	DIP-5240GP-00N	F.01U.359.551	Management Appliance GPU wo HD
DIVAR IP all-in-one 5000	DIP-5244GP-4HD	F.01U.359.552	Management Appliance GPU 4x4TB
DIVAR IP all-in-one 5000	DIP-5248GP-4HD	F.01U.359.553	Management Appliance GPU 4x8TB

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4x12TB

Bosch DIVAR IP all-in-one 7000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7280-00N	F.01U.362.591	2U Management Appliance w/o HD
DIVAR IP all-in-one 7000	DIP-7284-8HD	F.01U.362.592	2U Management Appliance 8x4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	2U Management Appliance 8x8TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	2U Management Appliance 8x12TB
DIVAR IP all-in-one 7000	DIP-72G0-00N	F.01U.362.595	3U Management Appliance wo HDD
DIVAR IP all-in-one 7000	DIP-72G8-16HD	F.01U.362.596	3U Management Appliance 16x8TB
DIVAR IP all-	DIP-72GC-16HD	F.01U.362.597	3U Management

Family Name	CTN	SAP#	Material description
in-one 7000			Appliance 16x12T

Bosch DIVAR IP all-in-one 7000 R3

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.385.539	Management appliance 2U without HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.385.540	Management appliance 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-7388-8HD	F.01U.385.541	Management appliance 2U 8X8 TB
DIVAR IP all-in-one 7000	DIP-738C-8HD	F.01U.385.542	Management appliance 2U 8X12 TB
DIVAR IP all-in-one 7000	DIP-73G0-00N	F.01U.385.543	Management appliance 3U without HD
DIVAR IP all-in-one 7000	DIP-73G8-16HD	F.01U.385.544	Management appliance 3U 16X8TB

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-73GC-16HD	F.01U.385.545	Management appliance 3U 16X12 TB
