

Multiple Curl vulnerabilities in the Git for Windows component of Bosch DIVAR IP all-in-one Devices

BOSCH-SA-587194-BT

Advisory Information

Advisory ID: BOSCH-SA-587194-BT

CVE Numbers and CVSS v3.1 Scores:

[CVE-2023-46218](#)

Base Score: [6.5 \(Medium\)](#)

[CVE-2023-46219](#)

Base Score: [5.3 \(Medium\)](#)

[CVE-2024-2004](#)

Base Score: [3.5 \(Low\)](#)

[CVE-2024-2398](#)

Base Score: [8.6 \(High\)](#)

Published: 7 Aug 2024

Last Updated: 7 Aug 2024

Summary

DIVAR IP System Manager is a central user interface that provides an easy system setup, configuration and application software upgrades through an easily accessible web-based application.

Multiple Curl vulnerabilities in the Git for Windows component have been discovered in DIVAR IP System Manager versions prior to 2.3.2, affecting several Bosch DIVAR IP all-

in-one models.

Affected Products

Bosch DIVAR IP all-in-one 4000 (DIP-44xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Bosch DIVAR IP all-in-one 6000 (DIP-64xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Bosch DIVAR IP all-in-one 7000 (DIP-74xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Bosch DIVAR IP all-in-one 7000 R3 (DIP-73xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Bosch DIVAR IP all-in-one 7000 (DIP-72xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Bosch DIVAR IP all-in-one 5000 (DIP-52xx)

CVE-2023-46218, CVE-2023-46219, CVE-2024-2004, CVE-2024-2398

Version(s): < DIVAR IP System Manager 2.3.2

Solution and Mitigations

Solution: Software Update

Customers are advised to upgrade the DIVAR IP System Manager to 2.3.2 version or later to fix all vulnerabilities listed in this advisory. Refer to the DIVAR IP System Manager Release Notes for the most appropriate upgrade process for your devices.

Vulnerability Details

CVE-2023-46218

CVE description: This flaw allows a malicious HTTP server to set "super cookies" in curl

that are then passed back to more origins than what is otherwise allowed or possible. This allows a site to set cookies that then would get sent to different and unrelated sites and domains. It could do this by exploiting a mixed case flaw in curl's function that verifies a given cookie domain against the Public Suffix List (PSL). For example a cookie could be set with `domain=co.UK` when the URL used a lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.

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

Base Score: 6.5 (Medium)

CVE-2023-46219

When saving HSTS data to an excessively long file name, curl could end up removing all contents, making subsequent requests using that file unaware of the HSTS status they should otherwise use.

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

Base Score: 5.3 (Medium)

CVE-2024-2004

When a protocol selection parameter option disables all protocols without adding any then the default set of protocols would remain in the allowed set due to an error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext protocol which has been explicitly disabled. `curl --proto -all,-http http://curl.se` The flaw is only present if the set of selected protocols disables the entire set of available protocols, in itself a command with no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this to be low severity bug.

Problem Type:

[CWE-115 Misinterpretation of Input](#)

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

Base Score: 3.5 (Low)

CVE-2024-2398

When an application tells libcurl it wants to allow HTTP/2 server push, and the amount

of received headers for the push surpasses the maximum allowed limit (1000), libcurl aborts the server push. When aborting, libcurl inadvertently does not free all the previously allocated headers and instead leaks the memory. Further, this error condition fails silently and is therefore not easily detected by an application.

Problem Type:

[CWE-772 Missing Release of Resource after Effective Lifetime](#)

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

Base Score: 8.6 (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] Bosch 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

7 Aug 2024: Initial Publication

Appendix

Material Lists

Bosch DIVAR IP all-in-one 4000 (DIP-44xx)

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 4000	DIP-4420IG-00N	F.01U.404.040	Management appliance w/o HDD
DIVAR IP all-in-one 4000	DIP-4424IG-2HD	F.01U.404.041	Management appliance 2x4TB
DIVAR IP all-in-one 4000	DIP-4428IG-2HD	F.01U.404.042	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP-442IIG-2HD	F.01U.404.043	Management appliance 2x18TB

Bosch DIVAR IP all-in-one 6000 (DIP-64xx)

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 6000	DIP-6440IG-00N	F.01U.404.045	Management appliance 1U w/o HDD
DIVAR IP all-in-one 6000	DIP-6444IG-4HD	F.01U.404.046	Management appliance 1U 4x4TB
DIVAR IP all-in-one 6000	DIP-6448IG-4HD	F.01U.404.047	Management appliance 1U 4x8TB
DIVAR IP all-in-one 6000	DIP-644IIG-4HD	F.01U.404.048	Management appliance 1U 4x18TB

Bosch DIVAR IP all-in-one 7000 (DIP-74xx)

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 7000	DIP-74C0-00N	F.01U.417.248	Management appliance, 2U w/o HDD
DIVAR IP all-in-one 7000	DIP-74C4-8HD	F.01U.417.249	Management appliance, 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-74C8-8HD	F.01U.417.250	Management appliance, 2U 8X8TB

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 7000	DIP-74CI-8HD	F.01U.417.251	Management appliance, 2U 8X18TB
DIVAR IP all-in-one 7000	DIP-74CI-12HD	F.01U.417.252	Management appliance, 2U 12X18TB
DIVAR IP all-in-one 7000	DIP-74G0-00N	F.01U.417.253	Management appliance, 3U w/o HDD
DIVAR IP all-in-one 7000	DIP-74GI-16HD	F.01U.417.254	Management appliance, 3U 16X18TB

Bosch DIVAR IP all-in-one 7000 R3 (DIP-73xx)

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.385.533	Management appliance 2U without HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.385.540	Management appliance 2U 8X4TB

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

Bosch DIVAR IP all-in-one 7000 (DIP-72xx)

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 7000	DIP-7280-00N	F.01U.362.591	Management appliance 2U without HD

Family Name	CTN	SAP#	Material Description
DIVAR IP all-in-one 7000	DIP-7284-8HD	F.01U.362.592	Management appliance 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	Management appliance 2U 8X8 TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	Management appliance 2U 8X12 TB
DIVAR IP all-in-one 7000	DIP-72G0-00N	F.01U.362.595	Management appliance 3U without HD
DIVAR IP all-in-one 7000	DIP-72G8-16HD	F.01U.362.596	Management appliance 3U 16X8TB
DIVAR IP all-in-one 7000	DIP-72GC-16HD	F.01U.362.597	Management appliance, 3U 16X12 TB

Bosch DIVAR IP all-in-one 5000 (DIP-52xx)

Family Name	CTN	SAP#	Material Description
-------------	-----	------	----------------------

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
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4x12TB