Git for Windows Multiple Security Vulnerabilities in Bosch DIVAR IP all-in-one Devices

BOSCH-SA-637386-BT

Advisory Information

Advisory ID: BOSCH-SA-637386-BT
CVE Numbers and CVSS v3.1 Scores: This information has been omitted for better readability. Please refer to section "Vulnerability Details" for the complete CVE list.
Published: 06 Mar 2024
Last Updated: 06 Mar 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 Git for Windows vulnerabilities have been discovered in DIVAR IP System Manager versions prior to 2.3.0, affecting several Bosch DIVAR IP all-in-one models.

Affected Products

Bosch DIVAR IP all-in-one 4000 (DIP-44xx)
  Version(s): < DIVAR IP System Manager 2.3.0
Bosch DIVAR IP all-in-one 5000 (DIP-52xx)
  Version(s): < DIVAR IP System Manager 2.3.0
Bosch DIVAR IP all-in-one 6000 (DIP-64xx)

Version(s): < DIVAR IP System Manager 2.3.0
Bosch DIVAR IP all-in-one 7000 (DIP-72xx)
Version(s): < DIVAR IP System Manager 2.3.0
Bosch DIVAR IP all-in-one 7000 R3 (DIP-73xx)
Version(s): < DIVAR IP System Manager 2.3.0

Solution and Mitigations

Software Update

Customers are advised to upgrade the DIVAR IP System Manager to 2.3.0 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-2021-21300

CVE description: Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS+ or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaound, if symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. *before* cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.

Problem Type:
CWE-59 Improper Link Resolution Before File Access ('Link Following')
CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N
Base Score: 8.0 (High)

CVE-2021-40330

CVE description: git_connect_git in connect.c in Git before 2.30.1 allows a repository path to contain a newline character, which may result in unexpected cross-protocol requests, as demonstrated by the git://localhost:1234/%0d%0a%0d%0aGET%20/%20HTTP/1.1 substring.

CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Base Score: 7.5 (High)

CVE-2022-23521

CVE description: Git is distributed revision control system. gitattributes are a mechanism to allow defining attributes for paths. These attributes can be defined by adding a `.gitattributes` file to the repository, which contains a set of file patterns and the attributes that should be set for paths matching this pattern. When parsing gitattributes, multiple integer overflows can occur when there is a huge number of path patterns, a huge number of attributes for a single pattern, or when the declared attribute names are huge. These overflows can be triggered via a crafted `.gitattributes` file that may be part of the commit history. Git silently splits lines longer than 2KB when parsing gitattributes from a file, but not when parsing them from the index. Consequentially, the failure mode depends on whether the file exists in the working tree, the index or both. This integer overflow can result in arbitrary heap reads and writes, which may result in remote code execution. The problem has been patched in the versions published on 2023-01-17, going back to v2.30.7. Users are advised to upgrade. There are no known workarounds for this issue.

Problem Type:
CWE-190: Integer Overflow or Wraparound
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Base Score: 9.8 (Critical)

CVE-2022-24765

CVE description: Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder `C:\.git` , which would be picked up by Git operations run supposedly

outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash users who set `GIT_PS1_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-gitare vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config` . Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access from those folders as a workaround. Alternatively, define or extend `GIT_CEILING_DIRECTORIES` to cover the *parent* directory of the user profile, e.g. `C:\Users` if the user profile is located in `C:\Users\my-user-name` .

Problem Type:
CWE-427: Uncontrolled Search Path Element
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N
Base Score: 6.0 (Medium)

CVE-2022-24767

CVE description: GitHub: Git for Windows' uninstaller vulnerable to DLL hijacking when run under the SYSTEM user account.

Problem Type:
CWE-427
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-2022-24975

CVE description: The –mirror documentation for Git through 2.35.1 does not mention the availability of deleted content, aka the "GitBleed" issue. This could present a security risk if information-disclosure auditing processes rely on a clone operation without the –mirror option.

Problem Type:
CWE-668
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Base Score: 7.5 (High)

CVE-2022-39253

CVE description: Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user` .

Problem Type:
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Base Score: 5.5 (Medium)

CVE-2022-39260

CVE description: Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()` , it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5,

2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround.

Problem Type:
CWE-787: Out-of-bounds Write
CWE-122: Heap-based Buffer Overflow
CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
Base Score: 8.5 (High)

CVE-2022-41903

CVE description: Git is distributed revision control system. `git log` can display commits in an arbitrary format using its `--format` specifiers. This functionality is also exposed to `git archive` via the `export-subst` gitattribute. When processing the padding operators, there is a integer overflow in `pretty.c::format_and_pad_commit()` where a `size_t` is stored improperly as an `int`, and then added as an offset to a `memcpy()`. This overflow can be triggered directly by a user running a command which invokes the commit formatting machinery (e.g., `git log --format=...`). It may also be triggered indirectly through git archive via the export-subst mechanism, which expands format specifiers inside of files within the repository during a git archive. This integer overflow can result in arbitrary heap writes, which may result in arbitrary code execution. The problem has been patched in the versions published on 2023-01-17, going back to v2.30.7. Users are advised to upgrade. Users who are unable to upgrade should disable `git archive` in untrusted repositories. If you expose git archive via `git daemon`, disable it by running `git config --global daemon.uploadArch false`.

Problem Type:
CWE-190: Integer Overflow or Wraparound
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Base Score: 9.8 (Critical)

CVE-2022-41953

CVE description: Git GUI is a convenient graphical tool that comes with Git for Windows. Its target audience is users who are uncomfortable with using Git on the command-line. Git GUI has a function to clone repositories. Immediately after the local clone is available, Git GUI will automatically post-process it, among other things running a spell checker called `aspell.exe` if it was found. Git GUI is implemented as a

Tcl/Tk script. Due to the unfortunate design of Tcl on Windows, the search path when looking for an executable *always includes the current directory* . Therefore, malicious repositories can ship with an `aspell.exe` in their top-level directory which is executed by Git GUI without giving the user a chance to inspect it first, i.e. running untrusted code. This issue has been addressed in version 2.39.1. Users are advised to upgrade. Users unable to upgrade should avoid using Git GUI for cloning. If that is not a viable option, at least avoid cloning from untrusted sources.

Problem Type:
CWE-426: Untrusted Search Path
CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
Base Score: 8.6 (High)

CVE-2023-22490

CVE description: Git is a revision control system. Using a specially-crafted repository, Git prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8 can be tricked into using its local clone optimization even when using a non-local transport. Though Git will abort local clones whose source `$GIT_DIR/objects` directory contains symbolic links, the `objects` directory itself may still be a symbolic link. These two may be combined to include arbitrary files based on known paths on the victim's filesystem within the malicious repository's working copy, allowing for data exfiltration in a similar manner as CVE-2022-39253.

A fix has been prepared and will appear in v2.39.2 v2.38.4 v2.37.6 v2.36.5 v2.35.7 v2.34.7 v2.33.7 v2.32.6, v2.31.7 and v2.30.8. If upgrading is impractical, two short-term workarounds are available. Avoid cloning repositories from untrusted sources with `--recurse-submodules` . Instead, consider cloning repositories without recursively cloning their submodules, and instead run `git submodule update` at each layer. Before doing so, inspect each new `.gitmodules` file to ensure that it does not contain suspicious module URLs.

Problem Type:
CWE-59: Improper Link Resolution Before File Access ('Link Following')
CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Base Score: 5.5 (Medium)

CVE-2023-22743

CVE description: Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, by carefully crafting DLL and putting into a subdirectory of a specific name living next to the Git for Windows installer, Windows can be tricked into side-loading said DLL. This potentially allows users with local write access to place malicious payloads in a location where automated upgrades might run the Git for Windows installer with elevation. Version 2.39.2 contains a patch for this issue. Some workarounds are available. Never leave untrusted files in the Downloads folder or its sub-folders before executing the Git for Windows installer, or move the installer into a different directory before executing it.

Problem Type:
CWE-426: Untrusted Search Path
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H
Base Score: 7.2 (High)

CVE-2023-23618

CVE description: Git for Windows is the Windows port of the revision control system Git. Prior to Git for Windows version 2.39.2, when `gitk` is run on Windows, it potentially runs executables from the current directory inadvertently, which can be exploited with some social engineering to trick users into running untrusted code. A patch is available in version 2.39.2. As a workaround, avoid using `gitk` (or Git GUI's "Visualize History" functionality) in clones of untrusted repositories.

Problem Type:
CWE-426: Untrusted Search Path
CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
Base Score: 8.6 (High)

CVE-2023-23946

CVE description: Git, a revision control system, is vulnerable to path traversal prior to versions 2.39.2, 2.38.4, 2.37.6, 2.36.5, 2.35.7, 2.34.7, 2.33.7, 2.32.6, 2.31.7, and 2.30.8. By feeding a crafted input to `git apply` , a path outside the working tree can be overwritten as the user who is running `git apply` . A fix has been prepared and will appear in v2.39.2, v2.38.4, v2.37.6, v2.36.5, v2.35.7, v2.34.7, v2.33.7, v2.32.6, v2.31.7, and v2.30.8. As a workaround, use `git apply --stat` to inspect a patch before applying; avoid applying one that creates a symbolic link and then creates a file beyond

the symbolic link.

Problem Type:
CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Base Score: 6.2 (Medium)

CVE-2023-25652

CVE description: Git is a revision control system. Prior to versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1, by feeding specially crafted input to `git apply --reject` , a path outside the working tree can be overwritten with partially controlled contents (corresponding to the rejected hunk(s) from the given patch). A fix is available in versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1. As a workaround, avoid using `git apply` with `--reject` when applying patches from an untrusted source. Use `git apply --stat` to inspect a patch before applying; avoid applying one that create a conflict where a link corresponding to the `*.rej` file exists.

Problem Type:
CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Base Score: 7.5 (High)

CVE-2023-25815

CVE description: In Git for Windows, the Windows port of Git, no localized messages are shipped with the installer. As a consequence, Git is expected not to localize messages at all, and skips the gettext initialization. However, due to a change in MINGW-packages, the `gettext()` function’s implicit initialization no longer uses the runtime prefix but uses the hard-coded path `C:\mingw64\share\locale` to look for localized messages. And since any authenticated user has the permission to create folders in `C:\` (and since `C:\mingw64` does not typically exist), it is possible for low-privilege users to place fake messages in that location where `git.exe` will pick them up in version 2.40.1.

This vulnerability is relatively hard to exploit and requires social engineering. For example, a legitimate message at the end of a clone could be maliciously modified to ask the user to direct their web browser to a malicious website, and the user might think that the message comes from Git and is legitimate. It does require local write access by the attacker, though, which makes this attack vector less likely. Version 2.40.1 contains a patch for this issue. Some workarounds are available. Do not work on a Windows machine with shared accounts, or alternatively create a `C:\mingw64` folder and leave it empty. Users who have administrative rights may remove the permission to create folders in `C:\` .

Problem Type:
CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)
CWE-134: Use of Externally-Controlled Format String
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:L/A:L
Base Score: 3.3 (Low)

CVE-2023-29007

CVE description: Git is a revision control system. Prior to versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1, a specially crafted `.gitmodules` file with submodule URLs that are longer than 1024 characters can used to exploit a bug in `config.c::git_config_copy_or_rename_section_in_file()` . This bug can be used to inject arbitrary configuration into a user’s `$GIT_DIR/config` when attempting to remove the configuration section associated with that submodule. When the attacker injects configuration values which specify executables to run (such as `core.pager` , `core.editor` , `core.sshCommand` , etc.) this can lead to a remote code execution. A fix A fix is available in versions 2.30.9, 2.31.8, 2.32.7, 2.33.8, 2.34.8, 2.35.8, 2.36.6, 2.37.7, 2.38.5, 2.39.3, and 2.40.1. As a workaround, avoid running `git submodule deinit` on untrusted repositories or without prior inspection of any submodule sections in `$GIT_DIR/config` .

Problem Type:
CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component (‘Injection’)
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Base Score: 7.0 (High)

CVE-2023-29011

CVE description: Git for Windows, the Windows port of Git, ships with an executable called `connect.exe`, which implements a SOCKS5 proxy that can be used to connect e.g. to SSH servers via proxies when certain ports are blocked for outgoing connections. The location of `connect.exe`'s config file is hard-coded as `/etc/connectrc` which will typically be interpreted as `C:\etc\connectrc`. Since `C:\etc` can be created by any authenticated user, this makes `connect.exe` susceptible to malicious files being placed there by other users on the same multi-user machine. The problem has been patched in Git for Windows v2.40.1. As a workaround, create the folder `etc` on all drives where Git commands are run, and remove read/write access from those folders. Alternatively, watch out for malicious `<drive>:\etc\connectrc` files on multi-user machines.

Problem Type:
CWE-427: Uncontrolled Search Path Element
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H
Base Score: 7.5 (High)

CVE-2023-29012

CVE description: Git for Windows is the Windows port of Git. Prior to version 2.40.1, any user of Git CMD who starts the command in an untrusted directory is impacted by an Uncontrolles Search Path Element vulnerability. Maliciously-placed `doskey.exe` would be executed silently upon running Git CMD. The problem has been patched in Git for Windows v2.40.1. As a workaround, avoid using Git CMD or, if using Git CMD, avoid starting it in an untrusted directory.

Problem Type:
CWE-427: Uncontrolled Search Path Element
CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H
Base Score: 7.2 (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

06 Mar 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-	DIP-644IIG-4HD	F.01U.404.048	Management

Family Name	CTN	SAP#	Material Description
in-one 6000			appliance 1U 4x18TB

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
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

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	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 5000 (DIP-52xx)

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

Family Name	CTN	SAP#	Material Description
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