# Unquoted Service Path Enumeration on SMCWatchDog Agent

BOSCH-SA-904062-BT

## Advisory Information

**Advisory ID:** BOSCH-SA-904062-BT
**CVE Numbers and CVSS v3.1 Scores:**
BOSCH-SA-904062-BT
Base Score: 7.8 (High)
**Published:** 15 Jan 2025
**Last Updated:** 15 Jan 2025

## Summary

An unquoted service path enumeration vulnerability on SMCWatchDog agent has been found affecting the DIVAR IP all-in-one 7000 (DIP-72xx) devices. This vulnerability can allow a local attacker to gain elevated privileges.

## Affected Products

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

## Solution and Mitigations

### Mitigation

Customers are advised to apply the following procedure to manually add quotation marks to the SMCWatchDog service path:

Open Registry Editor (regedit)
Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Supermicro Watchdog Agent
On the right pane double-click on the Image-Path configuration
Update the Value data from C:\Program Files (x86)\SuperMicro\Watchdog\SMCWatchDog.exe to "C:\Program Files (x86)\SuperMicro\Watchdog\SMCWatchDog.exe" (add quotes to beginning and end)
Click Ok

In order to confirm the correct configuration of the SMCWatchDog service path, please carry on the following steps:

Open *Services*
Double-click the *Supermicro Watchdog Agent* service from the list
Check that the Path to executable is quoted: *"C:\Program Files (x86)\SuperMicro\Watchdog\SMCWatchDog.exe"*

# Vulnerability Details

## BOSCH-SA-904062-BT

The SuperMicro Watchdog Agent uses an unquoted service path, which contains at least one whitespace character that could allow a local attacker to gain elevated privileges on the system.

Problem Type:
CWE-428: Unquoted Search Path or Element

# 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] Public Advisory: https://psirt.bosch.com/security-advisories/BOSCH-SA-904062-BT.html

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

# Revision History

15 Jan 2025: Initial Publication

# Appendix

## Material Lists

### 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-in-one 7000 | DIP-72GC-16HD | F.01U.362.597 | 3U Management Appliance 16x12TB |