



# CVE-2022-28620

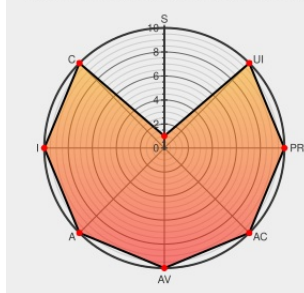
Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

## CVE-2022-28620

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Cray Ex Supercomputers](#) from [Hpe](#) contain the following vulnerability:

A remote authentication bypass vulnerability was discovered in HPE Cray Legacy Shasta System Solutions; HPE Slingshot; and HPE Cray EX supercomputers versions: Prior to node controller firmware associated with HPE Cray EX liquid cooled blades, and all versions of chassis controller firmware associated with HPE Cray EX liquid cooled cabinets prior to 1.6.27/1.5.33/1.4.27; All Slingshot versions prior to 1.7.2; All versions of node controller firmware associated with HPE Cray EX liquid cooled blades, and all versions of chassis controller firmware associated with HPE Cray EX liquid cooled cabinets prior to 1.6.27/1.5.33/1.4.27. HPE has provided a software update to resolve this vulnerability in HPE Cray Legacy Shasta System Solutions, HPE Slingshot, and HPE Cray EX Supercomputers.

CVE-2022-28620 has been assigned by [security-alert@hpe.com](mailto:security-alert@hpe.com) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

CVE References

| Description                           | Tags                                                         | Link                                                                                                            |
|---------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Document Display   HPE Support Center | <a href="#">support.hpe.com</a><br><a href="#">text/html</a> | <a href="#">MISC support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=emr_na-hpesbcr04284en_us</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3)                                                                          |        |                                                                   |         |        |         |          |
|-------------------------------------------------------------------------------------------------------------------|--------|-------------------------------------------------------------------|---------|--------|---------|----------|
| Type                                                                                                              | Vendor | Product                                                           | Version | Update | Edition | Language |
| Hardware <br><a href="#">↗</a>   | Hpe    | Cray Ex Supercomputers                                            | -       | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Ex Supercomputers Firmware                                   | 1.4.27  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Ex Supercomputers Firmware                                   | 1.5.33  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Ex Supercomputers Firmware                                   | 1.6.27  | All    | All     | All      |
| Hardware <br><a href="#">↗</a> | Hpe    | Cray Sh Supercomputer Air Cooled Base System Code                 | -       | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Air Cooled Base System Code Firmware        | 1.4.27  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Air Cooled Base System Code Firmware        | 1.5.33  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Air Cooled Base System Code Firmware        | 1.6.27  | All    | All     | All      |
| Hardware <br><a href="#">↗</a> | Hpe    | Cray Sh Supercomputer Liquid Cooled Base System Code              | -       | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Base System Code Firmware     | 1.4.27  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Base System Code Firmware     | 1.5.33  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Base System Code Firmware     | 1.6.27  | All    | All     | All      |
| Hardware <br><a href="#">↗</a> | Hpe    | Cray Sh Supercomputer Liquid Cooled Tds Base System Code          | -       | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Tds Base System Code Firmware | 1.4.27  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Tds Base System Code Firmware | 1.5.33  | All    | All     | All      |
| Operating System                                                                                                  | Hpe    | Cray Sh Supercomputer Liquid Cooled Tds Base System Code Firmware | 1.6.27  | All    | All     | All      |

|                                                                                                   |     |                                                                   |        |     |     |     |
|---------------------------------------------------------------------------------------------------|-----|-------------------------------------------------------------------|--------|-----|-----|-----|
| Operating System                                                                                  | Hpe | Cray Sh Supercomputer Liquid Cooled Ids Base System Code Firmware | 1.6.2/ | All | All | All |
| Hardware         | Hpe | Slingshot                                                         | -      | All | All | All |
| Operating System                                                                                  | Hpe | Slingshot Firmware                                                | All    | All | All | All |
| cpe:2.3:h:hpe:cray_ex_supercomputers:-:*:*:*:*:*:                                                 |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_ex_supercomputers_firmware:1.4.27:*:*:*:*:*:                                   |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_ex_supercomputers_firmware:1.5.33:*:*:*:*:*:                                   |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_ex_supercomputers_firmware:1.6.27:*:*:*:*:*:                                   |     |                                                                   |        |     |     |     |
| cpe:2.3:h:hpe:cray_sh_supercomputer_air_cooled_base_system_code:-:*:*:*:*:*:                      |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_air_cooled_base_system_code_firmware:1.4.27:*:*:*:*:*:        |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_air_cooled_base_system_code_firmware:1.5.33:*:*:*:*:*:        |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_air_cooled_base_system_code_firmware:1.6.27:*:*:*:*:*:        |     |                                                                   |        |     |     |     |
| cpe:2.3:h:hpe:cray_sh_supercomputer_liquid_cooled_base_system_code:-:*:*:*:*:*:                   |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_base_system_code_firmware:1.4.27:*:*:*:*:*:     |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_base_system_code_firmware:1.5.33:*:*:*:*:*:     |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_base_system_code_firmware:1.6.27:*:*:*:*:*:     |     |                                                                   |        |     |     |     |
| cpe:2.3:h:hpe:cray_sh_supercomputer_liquid_cooled_tds_base_system_code:-:*:*:*:*:*:               |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_tds_base_system_code_firmware:1.4.27:*:*:*:*:*: |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_tds_base_system_code_firmware:1.5.33:*:*:*:*:*: |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:cray_sh_supercomputer_liquid_cooled_tds_base_system_code_firmware:1.6.27:*:*:*:*:*: |     |                                                                   |        |     |     |     |
| cpe:2.3:h:hpe:slingshot:-:*:*:*:*:*:                                                              |     |                                                                   |        |     |     |     |
| cpe:2.3:o:hpe:slingshot_firmware:*:*:*:*:*:                                                       |     |                                                                   |        |     |     |     |

No vendor comments have been submitted for this CVE

| Social Mentions                                                                                    |                                                                                                                                                                                                                |                     |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Source                                                                                             | Title                                                                                                                                                                                                          | Posted (UTC)        |
|  @autumn_good_35 | スパコンの水冷関連のコントローラーで認証バイパス。 CVE-2022-28620 HPESBCR04284 rev.1 - HPE Cray EX Supercomputers, Cray Shasta System Solut... <a href="https://twitter.com/i/web/status/1561111111">twitter.com/i/web/status/1...</a>  | 2022-06-20 02:29:48 |
|  @CVEreport      | CVE-2022-28620 : A remote authentication bypass vulnerability was discovered in #HPE Cray Legacy Shasta System Solu... <a href="https://twitter.com/i/web/status/1561111111">twitter.com/i/web/status/1...</a> | 2022-06-24 15:19:16 |
|  /r/netcve       | <a href="#">CVE-2022-28620</a>                                                                                                                                                                                 | 2022-06-24 16:22:16 |

[← Previous ID](#)[Next ID→](#)

© [CVE.report](#) 2023  |

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](#)