



HCL AION is affected by a Cacheable HTTP Response vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-52659 |
| State | PUBLISHED |
| Assigner | HCL |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-01-19 18:16:03 UTC |
| Updated | 2026-04-25 18:04:34 UTC |
| Description | HCL AION version 2 is affected by a Cacheable HTTP Response vulnerability. This may lead to unintended storage of sensitive information. |

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.000420000 probability, percentile 0.128130000 (date 2026-04-25)

Problem Types: CWE-525 | CWE-525 CWE-525: Use of Web Browser Cache Containing Sensitive Information

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| 3.1 | psirt@hcl.com | Secondary | 2.8 | LOW | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L |
| 3.1 | CNA | CVSS | 2.8 | LOW | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Hcltech | Aion | 2.0.0 | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------------|---------|------------|---------------|
| CNA | HCL Software | AION | affected 2 | Not specified |

References

| Reference | Source | Link | Tags |
|-------------------------------------|---------------|--------------------------|---------------------|
| support.hcl-software.com/kb_view.do | psirt@hcl.com | support.hcl-software.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)