



# CVE-2005-2670

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2005-2670                                                                                                              |
| State           | PUBLISHED                                                                                                                  |
| Assigner        | mitre                                                                                                                      |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                               |
| Published       | 2005-08-23 04:00:00 UTC                                                                                                    |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                    |
| Description     | Directory traversal vulnerability in HAURI Anti-Virus products including ViRobot Expert 4.0, Advanced Server, Linux Server |

## Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:N

Problem Types: NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product  | Version | Update | Edition | Language |
|-------------|--------|----------|---------|--------|---------|----------|
| Application | Hauri  | Livecall | All     | All    | All     | All      |

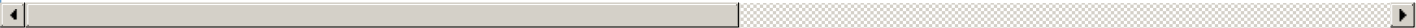
|             |                       |                                         |     |     |     |     |
|-------------|-----------------------|-----------------------------------------|-----|-----|-----|-----|
| Application | <a href="#">Hauri</a> | <a href="#">Virobot Advanced Server</a> | All | All | All | All |
| Application | <a href="#">Hauri</a> | <a href="#">Virobot Expert</a>          | 4.0 | All | All | All |
| Application | <a href="#">Hauri</a> | <a href="#">Virobot Linux Server</a>    | 2.0 | All | All | All |

Vendor Declared Affected Products

| Source | Vendor             | Product             | Version      | Platforms     |
|--------|--------------------|---------------------|--------------|---------------|
| CNA    | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

References

| Reference                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------|
| 404 Not Found                                                                                                                          |
| SecurityTracker.com Archives - HAURI ViRobot Input Validation Hole in Processing Compressed Archive Contents Lets Remote Users Write / |
| Secunia - Advisories - HAURI Anti-Virus Compressed Archive Directory Traversal                                                         |
| About Secunia Research   Flexera                                                                                                       |
| HAURI Anti-Virus Compressed Files Directory Traversal Vulnerability                                                                    |
| CVE Program record                                                                                                                     |
| NVD vulnerability detail                                                                                                               |



No vendor comments have been submitted for this CVE.

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