



# CVE-2007-3908

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2007-3908                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2007-07-19 17:30:00 UTC                                                                                                  |
| <b>Updated</b>         | 2018-10-15 21:32:00 UTC                                                                                                  |
| <b>Description</b>     | Unspecified vulnerability in HP ServiceGuard for Linux for Red Hat Enterprise Linux (RHEL) 2.1 SG A.11.14.04 through A.1 |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor             | Product                                | Version    | Update | Edition | Language |
|-------------|--------------------|----------------------------------------|------------|--------|---------|----------|
| Application | <a href="#">Hp</a> | <a href="#">Cluster Object Manager</a> | b.03.01.02 | All    | All     | All      |
| Application | <a href="#">Hp</a> | <a href="#">Cluster Object Manager</a> | b.03.01.02 | All    | All     | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.04 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.05 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.06 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.04 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.05 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.07 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.08 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.09 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.10 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.04 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.05 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.14.06 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.04 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.05 | All    | rhel    | All      |
| Application | <a href="#">Hp</a> | <a href="#">Serviceguard</a>           | a.11.16.07 | All    | rhel    | All      |

|             |    |              |            |     |      |     |
|-------------|----|--------------|------------|-----|------|-----|
| Application | Hp | Serviceguard | a.11.16.08 | All | rhel | All |
| Application | Hp | Serviceguard | a.11.16.09 | All | rhel | All |
| Application | Hp | Serviceguard | a.11.16.10 | All | rhel | All |

| References                                                                            |         |  |                                                                      |           |  |  |
|---------------------------------------------------------------------------------------|---------|--|----------------------------------------------------------------------|-----------|--|--|
| Reference                                                                             | Source  |  | Link                                                                 | Tags      |  |  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                      | VUPEN   |  | <a href="http://www.vupen.com">www.vupen.com</a>                     |           |  |  |
| HP ServiceGuard Unspecified Privilege Escalation Vulnerability - Secunia.com          | SECUNIA |  | <a href="http://secunia.com">secunia.com</a>                         | Patch, Ve |  |  |
| HP Serviceguard for Linux Unspecified Local Privilege Escalation Vulnerability        | BID     |  | <a href="http://www.securityfocus.com">www.securityfocus.com</a>     |           |  |  |
| SecurityFocus                                                                         | HP      |  | <a href="http://www.securityfocus.com">www.securityfocus.com</a>     |           |  |  |
| 38159                                                                                 | OSVDB   |  | <a href="http://osvdb.org">osvdb.org</a>                             |           |  |  |
| CXSecurity - IDS                                                                      | SREASON |  | <a href="http://securityreason.com">securityreason.com</a>           |           |  |  |
| HP Serviceguard for Linux Lets Local Users Gain Elevated Privileges - SecurityTracker | SECTRAK |  | <a href="http://www.securitytracker.com">www.securitytracker.com</a> | Patch     |  |  |
| CVE Program record                                                                    | CVE.ORG |  | <a href="http://www.cve.org">www.cve.org</a>                         | canonical |  |  |
| NVD vulnerability detail                                                              | NVD     |  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       | canonical |  |  |

No vendor comments have been submitted for this CVE.

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