



# CVE-2011-1760

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

## Summary

|                        |                                                                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-1760                                                                                                                     |
| <b>State</b>           | PUBLIC                                                                                                                            |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                      |
| <b>Published</b>       | 2011-06-09 19:55:00 UTC                                                                                                           |
| <b>Updated</b>         | 2011-09-07 03:16:00 UTC                                                                                                           |
| <b>Description</b>     | utils/opcontrol in OProfile 0.9.6 and earlier might allow local users to conduct eval injection attacks and gain privileges via s |

## Risk And Classification

### Problem Types: CWE-94

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                          | Product                  | Version | Update | Edition | Language |
|-------------|---------------------------------|--------------------------|---------|--------|---------|----------|
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.1     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.2     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.3     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.4     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.5     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.5.1   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.5.2   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.5.3   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.5.4   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.6     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.6.1   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.7     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.7.1   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.8     | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.8.1   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.8.2   | All    | All     | All      |
| Application | <a href="#">Maynard Johnson</a> | <a href="#">Oprofile</a> | 0.9     | All    | All     | All      |



|                                                                                                                                        |   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|
| oss-security - Re: CVE Request -- oprofile -- Local privilege escalation via crafted opcontrol event parameter when authorized by sudo | I |
| OProfile 'opcontrol' Utility 'set_event()' Local Privilege Escalation Vulnerability                                                    | I |
| oss-security - Re: CVE Request -- oprofile -- Local privilege escalation via crafted opcontrol event parameter when authorized by sudo | I |
| Debian -- Security Information -- DSA-2254-1 oprofile                                                                                  | I |
| oss-security - Re: CVE Request -- oprofile -- Local privilege escalation via crafted opcontrol event parameter when authorized by sudo | I |
| oss-security - Re: CVE Request -- oprofile -- Local privilege escalation via crafted opcontrol event parameter when authorized by sudo | I |
| Bug 700883 – CVE-2011-1760 oprofile: Local privilege escalation via crafted opcontrol event parameter                                  | C |
| Ubuntu update for oprofile - Secunia.com                                                                                               | S |
| oss-security - Re: CVE Request -- oprofile -- Local privilege escalation via crafted opcontrol event parameter when authorized by sudo | I |
| Debian update for oprofile - Secunia.com                                                                                               | S |
| USN-1166-1: OProfile vulnerabilities   Ubuntu                                                                                          | I |
| CVE Program record                                                                                                                     | C |
| NVD vulnerability detail                                                                                                               | I |



No vendor comments have been submitted for this CVE.

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