



# CVE-2010-3260

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

## Summary

|                        |                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-3260                                                                                                       |
| <b>State</b>           | PUBLIC                                                                                                              |
| <b>Assigner</b>        | cve@mitre.org                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                        |
| <b>Published</b>       | 2011-04-27 00:55:00 UTC                                                                                             |
| <b>Updated</b>         | 2011-07-19 04:00:00 UTC                                                                                             |
| <b>Description</b>     | oxf/xml/xerces/XercesSAXParserFactoryImpl.java in the xforms-server component in the XForms service in Orbeon Forms |

## Risk And Classification

### Problem Types: CWE-264

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product               | Version | Update | Edition | Language |
|-------------|------------------------|-----------------------|---------|--------|---------|----------|
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 1.5     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.0     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.1     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.2     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.5     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.6     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.7     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.8     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.0     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.5     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.6     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.7.1   | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.8     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 1.5     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.0     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.1     | All    | All     | All      |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.2     | All    | All     | All      |

|             |                        |                       |       |     |     |     |
|-------------|------------------------|-----------------------|-------|-----|-----|-----|
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.5   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.6   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.7   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 2.8   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.0   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.5   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.6   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.7.1 | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | 3.8   | All | All | All |
| Application | <a href="#">Orbeon</a> | <a href="#">Forms</a> | All   | All | All | All |

| References                                                                                                      |         |                             |  |
|-----------------------------------------------------------------------------------------------------------------|---------|-----------------------------|--|
| Reference                                                                                                       | Source  | Link                        |  |
| Detica - Securing a Connected World                                                                             | MISC    | <a href="#">www.strats</a>  |  |
| Implemented "[ #315668 ] Disable loading of external entities in XML ... · orbeon/orbeon-forms@aba6681 · GitHub | CONFIRM | <a href="#">github.com</a>  |  |
| Orbeon Forms 3.9 - forms                                                                                        | CONFIRM | <a href="#">wiki.orbeon</a> |  |
| Orbeon Forms XML Injection Vulnerability                                                                        | BID     | <a href="#">www.secur</a>   |  |
| CVE Program record                                                                                              | CVE.ORG | <a href="#">www.cve.o</a>   |  |
| NVD vulnerability detail                                                                                        | NVD     | <a href="#">nvd.nist.go</a> |  |

No vendor comments have been submitted for this CVE.

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