



# CVE-2001-0949

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2001-0949                                                                                                              |
| <b>State</b>           | PUBLIC                                                                                                                     |
| <b>Assigner</b>        | cve@mitre.org                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2001-12-04 05:00:00 UTC                                                                                                    |
| <b>Updated</b>         | 2017-12-19 02:29:00 UTC                                                                                                    |
| <b>Description</b>     | Buffer overflows in forms.exe CGI program in ValiCert Enterprise Validation Authority (EVA) Administration Server 3.3 thro |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor   | Product                         | Version | Update | Edition | Language |
|-------------|----------|---------------------------------|---------|--------|---------|----------|
| Application | Valicert | Enterprise Validation Authority | 3.3     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.4     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.5     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.6     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.7     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.8     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.9     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 4.0     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 4.1     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 4.2     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 4.2.1   | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.3     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.4     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.5     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.6     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.7     | All    | All     | All      |
| Application | Valicert | Enterprise Validation Authority | 3.8     | All    | All     | All      |

|             |          |                                 |       |     |     |     |
|-------------|----------|---------------------------------|-------|-----|-----|-----|
| Application | Valicert | Enterprise Validation Authority | 3.9   | All | All | All |
| Application | Valicert | Enterprise Validation Authority | 4.0   | All | All | All |
| Application | Valicert | Enterprise Validation Authority | 4.1   | All | All | All |
| Application | Valicert | Enterprise Validation Authority | 4.2   | All | All | All |
| Application | Valicert | Enterprise Validation Authority | 4.2.1 | All | All | All |

| References                                                                                        |  |  |         |                                                                                |  |  |
|---------------------------------------------------------------------------------------------------|--|--|---------|--------------------------------------------------------------------------------|--|--|
| Reference                                                                                         |  |  | Source  | Link                                                                           |  |  |
| ValiCert Enterprise Validation Authority forms.exe mode Buffer Overflow Vulnerability             |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| 'NMRC Advisory - Multiple Valicert Problems' - MARC                                               |  |  | BUGTRAQ | <a href="http://marc.info">marc.info</a>                                       |  |  |
| ValiCert Enterprise Validation Authority forms.exe maxMsgLen Buffer Overflow Vulnerability        |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe nextUpdatePeriod Buffer Overflow Vulnerability |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe blockTime Buffer Overflow Vulnerability        |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe listenLength Buffer Overflow Vulnerability     |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe useExpiredCRLs Buffer Overflow Vulnerability   |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| IBM X-Force Exchange                                                                              |  |  | XF      | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |  |  |
| ValiCert Enterprise Validation Authority maxOCSPValidityPeriod Buffer Overflow Vulnerability      |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe Certificate_File Buffer Overflow Vulnerability |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe buildLocal Buffer Overflow Vulnerability       |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe extension Buffer Overflow Vulnerability        |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert                                                                                          |  |  | CONFIRM | <a href="http://www.valicert.com">www.valicert.com</a>                         |  |  |
| ValiCert Enterprise Validation Authority forms.exe maxConnPerSite Buffer Overflow Vulnerability   |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| 504 Gateway Time-out                                                                              |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority Private Key Generation Buffer Overflow Vulnerability     |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| ValiCert Enterprise Validation Authority forms.exe exitTime Buffer Overflow Vulnerability         |  |  | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |  |  |
| CVE Program record                                                                                |  |  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                                   |  |  |
| NVD vulnerability detail                                                                          |  |  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                 |  |  |

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)