# CVE-2003-0545

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2003-0545 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2003-11-17 05:00:00 UTC |
| **Updated** | 2025-04-03 01:03:51 UTC |
| **Description** | Double free vulnerability in OpenSSL 0.9.7 allows remote attackers to cause a denial of service (crash) and possibly execut |

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Problem Types:** CWE-415 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 10 | | AV:N/AC:L/Au:N/C:C/I:C/A:C |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Openssl | Openssl | 0.9.6 | All | All | All |
| Application | Openssl | Openssl | 0.9.7 | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source |
|---|---|
| CERT/CC Vulnerability Note VU#935264 | af854a3a-2127-422b-91 |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91 |
| Repository / Oval Repository | af854a3a-2127-422b-91 |
| OpenSSL ASN.1 Parsing Vulnerabilities | af854a3a-2127-422b-91 |
| IBM Vulnerability Detected: 170.23.146.40:443 - OpenSSL Overflow Via Invalid Certificate Passing - United States | af854a3a-2127-422b-91 |
| Webmail - OVH | af854a3a-2127-422b-91 |
| Debian -- Security Information -- DSA-394-1 openssl095 | af854a3a-2127-422b-91 |
| IBM Rational RequisitePro OpenSSL Vulnerability - Advisories - Secunia | af854a3a-2127-422b-91 |
| www.uniras.gov.uk/vuls/2003/006489/openssl.htm | af854a3a-2127-422b-91 |

| | |
|---|---|
| CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations | af854a3a-2127-422b-91 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Red Hat | 2008-07-07 | Mark J Cox | Not vulnerable. The OpenSSL packages in Red Hat Enterprise Linux 2.1 were not affected by th |

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