



# CVE-2010-3044

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

## Summary

|                        |                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2010-3044                                                                                                      |
| <b>State</b>           | PUBLIC                                                                                                             |
| <b>Assigner</b>        | psirt@cisco.com                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                       |
| <b>Published</b>       | 2011-02-02 23:00:00 UTC                                                                                            |
| <b>Updated</b>         | 2017-08-17 01:32:00 UTC                                                                                            |
| <b>Description</b>     | Multiple buffer overflows in the Cisco WebEx Recording Format (WRF) and Advanced Recording Format (ARF) Players T2 |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                                | Version      | Update | Edition | Language |
|-------------|--------|----------------------------------------|--------------|--------|---------|----------|
| Application | Cisco  | Webex Advanced Recording Format Player | 26.49        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.10        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.11.0.3328 | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.12        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.13        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 26.49        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.10        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.11.0.3328 | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.12        | All    | All     | All      |
| Application | Cisco  | Webex Advanced Recording Format Player | 27.13        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 26.49        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 27.10        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 27.11.0.3328 | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 27.12        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 27.13        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 26.49        | All    | All     | All      |
| Application | Cisco  | Webex Recording Format Player          | 27.10        | All    | All     | All      |

|             |       |                               |              |     |     |     |
|-------------|-------|-------------------------------|--------------|-----|-----|-----|
| Application | Cisco | Webex Recording Format Player | 27.11.0.3328 | All | All | All |
| Application | Cisco | Webex Recording Format Player | 27.12        | All | All | All |
| Application | Cisco | Webex Recording Format Player | 27.13        | All | All | All |

| References                                                                                    |  |  |          |                                                                                 |  |  |
|-----------------------------------------------------------------------------------------------|--|--|----------|---------------------------------------------------------------------------------|--|--|
| Reference                                                                                     |  |  | Source   | Link                                                                            |  |  |
| Cisco WebEx WRF and ARF File Format Multiple Remote Buffer Overflow Vulnerabilities           |  |  | BID      | <a href="http://www.securityfocus.com">www.securityfocus.com</a>                |  |  |
| IBM X-Force Exchange                                                                          |  |  | XF       | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |  |  |
| Cisco WebEx Player Buffer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker |  |  | SECTrack | <a href="https://securitytracker.com">securitytracker.com</a>                   |  |  |
| tools.cisco.com/security/center/viewAlert.x                                                   |  |  | CONFIRM  | <a href="https://tools.cisco.com">tools.cisco.com</a>                           |  |  |
| Cisco Security Advisory: Multiple Cisco WebEx Player Vulnerabilities - Cisco Systems          |  |  | CISCO    | <a href="http://www.cisco.com">www.cisco.com</a>                                |  |  |
| FortiGuard   Fortinet Discovers Multiple Vulnerabilities in Cisco WebEx Players               |  |  | MISC     | <a href="http://www.fortiguards.com">www.fortiguards.com</a>                    |  |  |
| CVE Program record                                                                            |  |  | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                                    |  |  |
| NVD vulnerability detail                                                                      |  |  | NVD      | <a href="https://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.