



CVE-2010-2838

Published on: 08/26/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

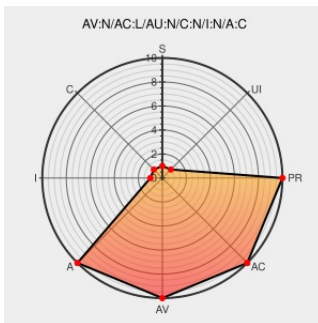
CVE-2010-2838

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Unified Communications Manager](#) from [Cisco](#) contain the following vulnerability:

The SendCombinedStatusInfo implementation in Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 7.0SU before 7.0(2a)SU3, 7.1 before 7.1(5), and 8.0 before 8.0(3) allows remote attackers to cause a denial of service (process failure) via a malformed SIP REGISTER message, aka Bug ID CSCtf66305.

CVE-2010-2838 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

COMPLETE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2010-2187](#)

Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service Vulnerabilities - Cisco Systems

[Patch](#)
[Vendor Advisory](#)
[www.cisco.com](#)
[text/html](#)

[CISCO 20100825 Cisco Unified Communications Manager Denial of Service Vulnerabilities](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	7.0(1)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.0(1)su1a	All	All	All
Application	Cisco	Unified Communications Manager	7.0(2)	All	All	All
Application	Cisco	Unified Communications Manager	7.0(2a)	All	All	All
Application	Cisco	Unified Communications Manager	7.0(2a)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.0\1\su1	All	All	All
Application	Cisco	Unified Communications Manager	7.0\1\su1a	All	All	All
Application	Cisco	Unified Communications Manager	7.0\2a\	All	All	All
Application	Cisco	Unified Communications Manager	7.0\2a\su1	All	All	All
Application	Cisco	Unified Communications Manager	7.0\2\	All	All	All
Application	Cisco	Unified Communications Manager	7.1(2a)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(2a)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1(2b)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(2b)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3a)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3a)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3a)su1a	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3b)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3b)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1(3b)su2	All	All	All
Application	Cisco	Unified Communications Manager	7.1(5)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(5)su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1(5a)	All	All	All
Application	Cisco	Unified Communications Manager	7.1(5b)	All	All	All
Application	Cisco	Unified Communications Manager	7.1\2a\	All	All	All
Application	Cisco	Unified Communications Manager	7.1\2a\su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1\2b\	All	All	All
Application	Cisco	Unified Communications Manager	7.1\2b\su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1\3a\	All	All	All
Application	Cisco	Unified Communications Manager	7.1\3a\su1	All	All	All
Application	Cisco	Unified Communications Manager	7.1\3a\su1a	All	All	All

[illegible]


```
cpe:2.3:a:cisco:unified_communications_manager:7.1(5a): : : : : :
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(5b):*:~::~
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(2a):*:~::~:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(2a)\su1:::*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((2b)\):*:~::~:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(2b)\su1.*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(3a)::*:.*:.*
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(3a)\su1:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((3a\)su1a:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\:(3b\:)*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((3b)\)su1:*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((3b\)su2.*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\(\3\):::*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((5a)\):*:~::~:*.*
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1\((5b)\):*:~::~:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(5):*:~::~:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.1(5)\su1:::*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(2c):*:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(2c)su1:*.:*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(3):*:~:*~*
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(2c):*:~::~:*.*
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(2c)\su1:::*.*.*.*.*.*
```

```
cpe:2.3:a:cisco:unified_communications_manager:8.0(3):*:*:*:*:*:*
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.0(1)\su1:::*:*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.0(1)\su1a:*.~::~.*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.0\((2a)\):*:~::~
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.0\((2a\)su1:::*:*:*:
```

```
cpe:2.3:a:cisco:unified_communications_manager:7.0(2):*:*:*:*:*
```

```
cpe:2.3:a:cisco:unified communications manager:7.1\((2a)\):*:~:~:~:~:~:~:
```

```
cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:*:*:
```

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report