

Cisco Security Advisory

# Cisco Unified Communications Manager DNA Interface Reflected Cross-Site Scripting Vulnerability



**Advisory ID:** Cisco-SA-20141103-CVE-2014-3373  
**Published:** 2014 November 3 18:17 GMT  
**Version 1.0:** Final  
**CVSS Score:** [Base - 4.3](#)  
**Workarounds:** [See below](#)  
**Cisco Bug IDs:** [CSCup92550](#)

[CVE-2014-3373](#)  
[CWE-79](#)  
[Download CVRF](#)  
[Download PDF](#)  
[Email](#)

## Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

## Subscribe to Cisco Security Notifications

[Subscribe](#)

### Summary

A vulnerability in the CCM Dialed Number Analyzer interface of the Cisco Unified Communications Manager Server contains a vulnerability that could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system.

The vulnerability is due to insufficient input validation of certain parameters passed via HTTP GET or POST methods.

Cisco has confirmed the vulnerability in a security notice and released software updates.

To exploit the vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

### Affected Products

Customers are advised to consult Cisco bug ID [CSCup92550](#) for a complete list of affected product versions.

### Vulnerable Products

At the time this alert was first published, Cisco Unified Communications Manager versions 9.1(2.10000.28) and prior were vulnerable. Later versions of Cisco Unified Communications Manager may also be vulnerable.

### Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

### Workarounds

Administrators are advised to apply the appropriate updates.

Users are advised not to visit websites or follow links that have suspicious characteristics or cannot be verified as safe.

For additional information about cross-site scripting attacks and the methods used to exploit these vulnerabilities, see the Cisco Applied Mitigation Bulletin [Understanding Cross-Site Scripting \(XSS\) Threat Vectors](#).

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

Administrators are advised to monitor affected systems.

### Fixed Software

Cisco customers with active contracts should contact their Cisco support team for assistance in upgrading to a software version that includes fixes for this vulnerability. Cisco customers without contracts may contact the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via email at [tac@cisco.com](mailto:tac@cisco.com) for assistance.

### Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

### URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20141103-CVE-2014-3373>

### Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2014-Nov-03

### Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.

<p><b>Information For</b></p> <ul style="list-style-type: none"> <li>Small Business</li> <li>Midsized Business</li> <li>Service Provider</li> <li>Executives</li> </ul> <p><b>Industries</b> &gt;</p> <p><b>Marketplace</b></p> <p><b>Contacts</b></p> <ul style="list-style-type: none"> <li>Contact Cisco</li> <li>Find a Reseller</li> </ul>	<p><b>News &amp; Alerts</b></p> <ul style="list-style-type: none"> <li>Newsroom</li> <li>Blogs</li> <li>Field Notices</li> <li>Security Advisories</li> </ul> <p><b>Technology Trends</b></p> <ul style="list-style-type: none"> <li>Cloud</li> <li>Internet of Things (IoT)</li> <li>Mobility</li> <li>Software Defined Networking (SDN)</li> </ul>	<p><b>Support</b></p> <ul style="list-style-type: none"> <li>Downloads</li> <li>Documentation</li> </ul> <p><b>Communities</b></p> <ul style="list-style-type: none"> <li>DevNet</li> <li>Learning Network</li> <li>Support Community</li> </ul> <p><b>Video Portal</b> &gt;</p>	<p><b>About Cisco</b></p> <ul style="list-style-type: none"> <li>Investor Relations</li> <li>Corporate Social Responsibility</li> <li>Environmental Sustainability</li> <li>Tomorrow Starts Here</li> <li>Our People</li> </ul> <p><b>Careers</b></p> <ul style="list-style-type: none"> <li>Search Jobs</li> <li>Life at Cisco</li> </ul> <p><b>Programs</b></p> <ul style="list-style-type: none"> <li>Cisco Designated VIP Program</li> <li>Cisco Powered</li> <li>Financing Options</li> </ul>
---	--	--	--