

Cisco Security Advisory

Cisco Desktop Collaboration Experience DX600 Series Potential Code Injection Vulnerability



Advisory ID: Cisco-SA-20130701-CVE-2013-3399 CVE-2013-3399 [Download CVRF](#)
Published: 2013 July 1 13:29 GMT CWE-94 [Download PDF](#)
Version 1.0: Final [Email](#)
CVSS Score: [Base - 6.0](#)
Workarounds: [See below](#)
Cisco Bug IDs: [CSCuf93957](#)
[CSCug22352](#)
[CSCug22462](#)

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 an underlying Android Application Programming Interface (API) utilized by the Cisco Desktop Collaboration Experience DX600 series endpoint could allow an authenticated, local attacker to inject code into the system.

The vulnerability is due to insufficient validation of specific values prior to their use to allocate a buffer. An attacker could exploit this vulnerability by overflowing a buffer. An exploit could allow the attacker to execute arbitrary code with elevated privileges.

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

To successfully exploit the vulnerability, the attacker would need to authenticate and have local access to the targeted system, which could limit the likelihood of an exploit.

Affected Products

Customers should refer to Cisco bug IDs [CSCuf93957](#), [CSCug22352](#), and [CSCug22462](#) for the most complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco Desktop Collaboration Experience DX650 Software versions 10.0(1) and prior were vulnerable. Later versions of Cisco Desktop Collaboration Experience DX650 Software may also be affected.

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.

Administrators are advised to allow only trusted users to access local systems.

Administrators are advised to apply the appropriate updates.

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 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-20130701-CVE-2013-3399>

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2013-Jul-01

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