Cisco Security Advisory

Cisco Desktop Collaboration Experience DX600 Series Potential Code Injection Vulnerability

Advisory ID: Cisco-SA-20130701-CVE-2013-3399
Published: 2013 July 1 13:29 GMT
Version1.0: Final
CVSS Score: Base - 6.0
Workarounds: See below
Cisco Bug IDs: CSCuf93957 CSCug22352 CSCug22462

CVE-2013-3399
CWE-94

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 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
