

Cisco Security Advisory

Sudo sudoedit Local Command Privilege Escalation Vulnerability



Advisory ID: Cisco-SA-20100419-CVE-2010-1163 CVE-2010-1163 [Download CVRF](#)
Last Updated: 2015 January 31 05:30 GMT CWE-264 [Download PDF](#)
Published: 2010 April 19 20:43 GMT [Email](#)
Version 5.0: Final
CVSS Score: [Base - 6.0](#)
Workarounds: [See below](#)

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

Sudo contains a vulnerability that could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges.

This vulnerability exists due to an error in the affected software while matching commands due to incorrect path resolution. A local attacker with privileges to run the `sudoedit` command could exploit this vulnerability to execute arbitrary commands with `root` privileges. An exploit could result in a complete system compromise.

Proof-of-concept code that exploits this vulnerability is publicly available.

The vendor has confirmed this vulnerability and released updated software.

To exploit the vulnerability, an attacker must have local access to the system and be granted special permissions to execute the `sudoedit` command. As a result of these requirements, the source of exploits are likely limited to current users of an affected system. Successful exploitation could allow a local attacker to execute arbitrary shell commands as `root`, leading to a full system compromise.

For this vulnerability to be successful, the attacker passes a command that has the `PATH` environment variable including a "." and not include any other directory that contains a `sudoedit` command. Also, a successful exploit requires the `ignore_dot` or `secure_path sudoers` options to be disabled.

Affected Products

Sudo has confirmed this vulnerability in a security advisory at the following link: [CVE-2010-1163](#)

Cisco has released Bug IDs at the following links: [CSCtg35974](#), [CSCth37846](#), [CSCtf18342](#), and [CSCth87771](#)

Red Hat has released a security advisory at the following link: [RHSA-2010:0361](#)

Vulnerable Products

Sudo versions 1.6.8 through 1.7.2p5 are 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.

Administrators are advised to restrict local access to trusted users.

Administrators are advised not to grant any `sudo` privileges to untrusted users.

Fixed Software

Sudo has released an updated version at the following link: [sudo 1.6.9p22, 1.7.2p6 or later](#)

CentOS packages can be updated using the `up2date` or `yum` command.

Red Hat packages can be updated using the `up2date` or `yum` command.

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-20100419-CVE-2010-1163>

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2010-Apr-19

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.

Information For

[Small Business](#)
[Midsize Business](#)
[Service Provider](#)
[Executives](#)

Industries >

Marketplace

Contacts

[Contact Cisco](#)
[Find a Reseller](#)

News & Alerts

[Newsroom](#)
[Blogs](#)
[Field Notices](#)
[Security Advisories](#)

Technology Trends

[Cloud](#)
[Internet of Things \(IoT\)](#)
[Mobility](#)
[Software Defined Networking \(SDN\)](#)

Support

[Downloads](#)
[Documentation](#)

Communities

[DevNet](#)
[Learning Network](#)
[Support Community](#)

Video Portal >

About Cisco

[Investor Relations](#)
[Corporate Social Responsibility](#)
[Environmental Sustainability](#)
[Tomorrow Starts Here](#)
[Our People](#)

Careers

[Search Jobs](#)
[Life at Cisco](#)

Programs

[Cisco Designated VIP Program](#)
[Cisco Powered](#)
[Financing Options](#)