

# Cisco Security Response: NAC Agent Installation Bypass

Document ID: 71210

<http://www.cisco.com/warp/public/707/cisco-sr-20060826-nac.shtml>

## Revision 1.0

For Public Release 2006 August 26 1900 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Cisco Response

This is the Cisco PSIRT response to the statements made by Andreas Gal and Joachim Feise in their advisory entitled "NAC agent installation bypass", available at

<http://www.securityfocus.com/archive/1/444424/30/0/threaded>

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

## Additional Information

The goal of the attack described in the advisory is to bypass the Operating System (OS) detection mechanisms available in the NAC (Network Admission Control) appliance software, in order to prevent the mandatory installation of the Cisco Clean Access (CCA) Agent. If the CCA Agent is not installed, machines that do not comply with the configured software policies will not be automatically patched/upgraded or quarantined on initial access to the network.

While it is possible to bypass the mandatory agent installation by following the steps in the advisory, it should be noted that:

- 1) Users cannot bypass authentication using the approach described in the advisory. Accordingly, unauthorized users (i.e., users with no credentials or invalid credentials) will not be able to gain access to the network using such approach.
- 2) If an administrator is concerned that users might attempt to bypass CCA Agent installation by masquerading a Windows machine as a non-Windows machine (e.g., Linux, MacOSX, etc.), the administrator can define Network Scanning rules on the CCA Manager and use network scans to perform additional OS-specific checks. This process should detect users attempting to masquerade their Windows machines as non-Windows machines.

Additional information on how to configure Network Scanning rules can be found in the Tech Note entitled

## [Clean Access – Use the Network Scanning Feature to Detect Users Who Attempt to Bypass Agent Checks.](#)

3) If a malicious user installs a personal firewall or similar software for the purpose of making the network scan time out, CCA provides options to quarantine such malicious users. Following such quarantine, administrators can then determine if users are attempting to masquerade their OS. Alternatively, network administrators can ask users to configure their personal firewalls to allow any traffic sourced from the Clean Access Server (CAS) IP address, so that it can successfully perform network scans.

4) Customers can also manually install either the CCA Agent software or the CCA Agent Installation stub (available in CCA version 4.0.0 and above) on end-user Windows machines, instead of using the OS detection routines. This will completely prevent the agent installation bypass described in the advisory from Andreas Gal and Joachim Feise.

## Revision History

Revision 1.0	2006 August 26	Initial public release.
--------------	----------------	-------------------------

## Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Aug 26, 2006

Document ID: 71210

---