

Cisco Security Response: NACATTACK Presentation

Document ID: 91196

<http://www.cisco.com/warp/public/707/cisco-sr-20070330-cta.sh>

Revision 1.0

For Public Release 2007 March 30 1445 UTC (GMT)

Please provide your feedback on this document.

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is Cisco PSIRT's response to the "NACATTACK" presentation by Dror-John Roecher and Michael Thumann, presented at Blackhat Europe on March 30th, 2007.

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 method of the attack is to simulate the communication between Cisco Trust Agent (CTA), a component of the Cisco Network Admission Control (NAC) Framework, and its interaction with network enforcement devices and Cisco Secure ACS.

Cisco NAC Framework supports both posture validation and authentication. Posture and authentication parameters are both credentials that can be used for making an admission decision. Cisco NAC Framework does not require posture information to authenticate incoming users as they access the network. In this regard, the CTA is only a messenger to transport posture credentials.

While it is possible to simulate the connection between CTA and Cisco Secure ACS and spoof posture information, it should be noted that this affects posture validation, not authentication. Customers can use user authentication, as well as device authentication through IEEE 802.1x. If authentication is used, users will not be able to bypass authentication using the approach described in the presentation. 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.

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.

Revision History

Revision 1.0	2007-Mar-30	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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 14, 2007

Document ID: 91196
