

# Cisco Security Notice: Alleged Bypassing Access Control List in Cisco IOS

Document ID: 52342

Alleged Bypassing Access Control List in Cisco IOS

## Revision 1.0

For Public Release 2004 May 27

---

Please provide your feedback on this document.

---

**Summary**

**Details**

**Status of This Notice: FINAL**

**Revision History**

**Cisco Security Procedures**

**Related Information**

---

## Summary

This Security Notice is to address the issue reported by Igor U. Miturin originally posted at <http://www.security.nnov.ru>. It was alleged that Access Control Lists (ACLs) can be bypassed by sending a TCP packet with RST and ACK flags set. After working with Mr. Miturin, it has been proven that this issue was a false alarm.

## Details

The original report by Mr Miturin indicated that in Cisco IOS® 11.2(11) it was possible to bypass the ACL by sending a TCP packet with RST and ACK flags set. This was originally posted (in Russian) at <http://www.security.nnov.ru/search/document.asp?docid=5974> and subsequently re-posted by several other Internet security portals and companies.

After working with Mr. Miturin, it has been proven that this issue was a false alarm. It is not possible to bypass an ACL with any packet and flag combination. 3ARA3A (the maintainer of [www.security.nnov.ru](http://www.security.nnov.ru) site) and ISS have removed reports from their sites.

## Status of This Notice: FINAL

This Notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty of any kind. Your use of the information on the Notice or materials linked from the Notice is at your own risk. Cisco reserves the right to change or update this notice at anytime.

# Revision History

Revision 1.0	2004-May-27	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>.

---

## Related Information

- <http://www.security.nnov.ru/search/document.asp?docid=5974> (in Russian)
  - <http://www.thebugs.ws/news/show.shtml?id=794>
  - <http://securitytracker.com/alerts/2004/Mar/1009570.html>
- 

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

---

Updated: May 27, 2004

Document ID: 52342

---