

# Table of Contents

<b><u>Cisco Security Notice: Response to BugTraq – TACACS+ Vulnerability</u></b> .....	1
<u>Revision 1.0</u> .....	1
<u>Last Updated 2000 May 30</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Details</u> .....	1
<u>Cisco Security Procedures</u> .....	2

# Cisco Security Notice: Response to BugTraq – TACACS+ Vulnerability

## Revision 1.0

Last Updated 2000 May 30

---

Please provide your feedback on this document.

---

**Summary**  
**Details**  
**Cisco Security Procedures**

---

## Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

## Details

Original Report: [http://www.openwall.com/advisories/OW-001-tac\\_plus.txt](http://www.openwall.com/advisories/OW-001-tac_plus.txt) . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/62745> .

```
To: BugTraq
Subject: Re: An Analysis of the TACACS+ Protocol and its Implementations
Date: May 30 2000 1:16PM
Author: Damir Rajnovic <drajnovi@cisco.com>
Message-ID: <4.2.0.58.20000530120817.00acec70@amsterdam.cisco.com>
In-Reply-To: <200005301059.OAA05030@false.com>
```

-----BEGIN PGP SIGNED MESSAGE-----

Hello,

We acknowledge that a buffer overflow mentioned in the analysis by Solar Designer is indeed present in an unsupported free version of TACACS+ server (officially it is a "developer's kit" and can be found at <http://cco/kobayashi/sw-center/access/tacacs-plus.html>) However, since that software is unsupported Cisco will not patch it. One can integrate the patch mentioned in Solar Designer's analysis, but Cisco will not be liable for any damage that it may cause. The unsupported patch can be found at <http://www.openwall.com/advisories/>

The above site and all its contents are not endorsed by Cisco in any way and we are declining any liability for a damage that may be caused if acted upon information presented on it. This link is included for completeness and convenience only.

Our commercial offerings CiscoSecure for Unix and NT are not vulnerable to the described overflow. If an oversized TACACS+ packet is sent to an IOS client, IOS will report an error as mentioned in the analysis and reject that packet. The device will continue to function normally and no service disruption will occur.

In order to utilize other TACACS+ protocol shortcomings as described in the brilliant analysis by Solar Designer, a culprit must have access to the path between the TACACS+ client and the server.

We would like to thank Solar Designer for sharing this analysis with us first and allowing us ample time to review our commercial products.

Regards,

Gaus

=====

Damir Rajnovic <psirt@cisco.com>, PSIRT Incident Manager, Cisco Systems  
<[http://www.cisco.com/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml)>  
Phone: +44 7715 546 033  
4 The Square, Stockley Park, Uxbridge, MIDDLESEX UB11 1BN, GB  
=====

There is no insolvable problems. Question remains: can you accept the solution?

-----BEGIN PGP SIGNATURE-----

Version: PGPfreeware 6.0.2i

iQCVAwUBOTOircAFeq0PniW5AQFYlwP/RdjJdljtCQwJA9sP+7odfBgZxxXRCmrv  
nzSQem9N7Ll6hV6tOA8ypopqhSzdH+eWbn/32dy1mmU1bH9cjXNaS9Fa21+mOtG8  
u2+kr/hnYzBwutFFzZFzsl1a4mg85G/u5twSs2U5RHqAWypAURYFE8W65431iIhno  
HD2oHDFGdcE=  
=iFx3

-----END PGP SIGNATURE-----

## 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/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml). 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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.