

Table of Contents

| | |
|--|---|
| <u>Cisco Security Notice: Response to BugTraq – Cisco Clean Access Agent (Perfigo) Bypass</u> | 1 |
| <u>Document ID: 66147</u> | 1 |
| <u>Revision 1.1</u> | 1 |
| <u>Last Updated 2005 November 07 1900 UTC (GMT)</u> | 1 |
| <u>For Public Release 2005 August 22 1600 UTC (GMT)</u> | 1 |
| <u>Please provide your feedback on this document</u> | 1 |
| <u>Summary</u> | 1 |
| <u>Details</u> | 1 |
| <u>Workarounds</u> | 3 |
| <u>Status of This Notice: FINAL</u> | 3 |
| <u>Revision History</u> | 4 |
| <u>Cisco Security Procedures</u> | 4 |
| <u>Related Information</u> | 4 |

Cisco Security Notice: Response to BugTraq – Cisco Clean Access Agent (Perfigo) Bypass

Document ID: 66147

Revision 1.1

Last Updated 2005 November 07 1900 UTC (GMT)

For Public Release 2005 August 22 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Details
Workarounds
Status of This Notice: FINAL
Revision History
Cisco Security Procedures
Related Information

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.

This notice is posted at <http://www.cisco.com/warp/public/707/cisco-sn-20050822-cca.shtml> .

Details

The original report is located at <http://www.securityfocus.com/archive/1/408603/30/0/threaded> .Cisco responded with the following:

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1
```

```
This is in response to the email posted by 'llhansen-bugtraq@adams.edu'  
on August 19, 2005.
```

```
The original email is available at  
http://www.securityfocus.com/archive/1/408603/30/0/threaded .
```

```
Attached: a cleartext, PGP signed version of this same email.
```

```
Hi llhansen,
```

While it is correct that a user can modify the 'User-Agent' string on access to the CCA Server authentication page in order to prevent installation of the CCA Agent, there are some things that should be clarified:

1) Users cannot bypass authentication irrespective of the value of the 'User-Agent' string provided. Hence, there is no danger of invalid users (users with no credentials or invalid credentials) getting onto the network.

2) If there is the suspicion that a malicious user might try to masquerade as non-Windows machines, e.g. Linux, in order to bypass CCA Agent installation, the administrator can define Network Scanning rules on the CCA Manager and use Nessus scans to determine the real OS in use. This will catch users that are masquerading. For this, the CCA administrator can either obtain the appropriate plug-ins from Tenable or www.nessus.org - as an alternative, users can write and integrate their own plugins.

3) Furthermore, if the malicious user installs a personal firewall or similar software, in order to make the network scan timeout, CCA provides options to quarantine the malicious user if the network scan times out. Hence, such users can also get quarantined, following which administrators can determine whether the user is masquerading or not.

CCA continues to evolve and include safeguards to prevent malicious users from trying to bypass the checks in place.

Thank you for your work on this problem. As always, working with the Cisco PSIRT team is the best way to verify the accuracy of information before posting it publicly.

We do greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist with Product Security Advisories. Our ultimate goal is to ensure that customers have accurate information on which to base upgrade and workaround decisions and we welcome partnership with researchers towards that goal.

Thanks,
Dario

Quidquid latine dictum sit, altum videtur

Dario Ciccarone
CCIE #10395
Product Security Incident Response Team (PSIRT)
Cisco Systems, Inc.
dciccaro@cisco.com

> -----Original Message-----
> From: llhansen-bugtraq@adams.edu [mailto:llhansen-bugtraq@adams.edu]
> Sent: Friday, August 19, 2005 12:30 PM
> To: bugtraq@securityfocus.com
> Subject: Cisco Clean Access Agent (Perfigo) bypass
>
> Description:
> Cisco Clean Access is an easily deployed software solution
> that can automatically detect, isolate, and clean infected or
> vulnerable devices that attempt to access your network. It
> identifies whether networked devices such as laptops,
> personal digital assistants, even game consoles are compliant
> with your network's security policies and repairs any

```
> vulnerabilities before permitting access to the network.
>
> Vendor site:
> http://www.cisco.com/en/US/products/ps6128/
>
> Affected versions:
> This works in at least 3.5.3.1 and 3.5.4.
>
> Discovery Date:
> 2005-08-12
>
> Report Date:
> 2005-08-19
>
> Severity:
> Medium
>
> Vulnerability:
> End users can bypass the "mandatory" installation of the
> Clean Access Agent by changing the User-Agent string of their
> browser. This allows them to connect to the network without
> the host-based checks being run. If configured, remote checks
> are still run.
>
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.1

iQA/AwUBQwni8IyVGB+6GuDwEQIruwCdF/lpHQcavH7KKntYk2RGLycAyPkAoN1W
J9PSvl9tU6lDJB39nR1Hiteg
=FrBo
-----END PGP SIGNATURE-----
```

Workarounds

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

Additional information about how to configure Network Scanning rules to detect malicious users trying to bypass the OS checks can be found in the document entitled "Clean Access – Use the Network Scanning Feature to Detect Users Who Attempt to Bypass Agent Checks", available at http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080545b62.shtml.

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Revision History

| | | |
|-----------------|-----------------------------|-------------------------------|
| Revision 1.1 | 2005–November–07 | Added workaround information. |
| Revision 1.0 | 2005–August–22 | 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>.

Related Information

- **Tech Note: Clean Access – Use the Network Scanning Feature to Detect Users Who Attempt to Bypass Agent Checks**
 - **Cisco Security Advisories and Notices**
-

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Nov 07, 2005

Document ID: 66147
