



More ▾

[Create Blog](#) [Sign In](#)

# malerisch.net

Security research, divulgations and food for thought.

[Home](#)

[Security Research](#)

[Advisories](#)

[Presentations](#)

[White Papers](#)

[Tools](#)

[Videos](#)

Thursday, 20 April 2017

## Trend Micro Threat Discovery Appliance - Session Generation Authentication Bypass (CVE-2016-8584)



[Tweet](#)



[Like 299](#)



[Share](#)

In the last few months, I have been testing several Trend Micro products with Steven Seeley ([@steventseeley](#)). Together, we have found more than 200+ RCE (Remote Code Execution) vulnerabilities and for the first time we presented the outcome of our research at [Hack In The Box 2017 Amsterdam](#) in April.

The presentation is available as a [PDF](#) or as a [Slideshare](#).

**About me**

[Public profile on LinkedIn](#)

[Google SERPs 'profile'](#)

[Previous Blog](#)

**Presentations** 14

I got 99 trend's and a # is all of them!

How we found over 100 200+ RCE vulnerabilities in Trend Micro software

**Documents** 0

**Infographics** 0

**Videos** 0

1 of 122

in

I got 99 trends and a # is all of them 4,271

Since it was not possible to cover all discovered vulnerabilities with a single presentation, this blog post will cover and analyze a further vulnerability that did not make it to the slides, and which affects the Trend Micro Threat Discovery Appliance (TDA) product.

### CVE-2016-8584 - TDA Session Generation Authentication Bypass

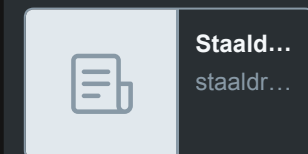
This was an interesting vulnerability, discovered after observing that two consecutive login attempts against the web interface returned the same session\_id token. Following this observation, our inference was that time factor played a role. After further analysis and reversing of the TDA libraries, the session management was found to be defined in the following library: /opt/TrendMicro/MinorityReport/lib/mini\_httpd/utils.so

## Tweets by @maleris

Roberto Suggi Retweeted

**Etienne Stalmans**  
@\_staaldrad

Here is my write-up of the new Git RCE vulnerability. Covers the process of discovery, stumbling, exploiting and disclosure. [staaldrad.github.io/post/2018-06-0...](https://staaldrad.github.io/post/2018-06-0...)



Jun 3, 2018

Roberto Suggi Retweeted

**Michał Bentkowski**  
@SecurityMB

Cisco recently fixed a bug I reported in ASA, see: [tools.cisco.com/security/ce](https://tools.cisco.com/security/ce)

Embed View on Twitter

Labels

Within this library, the `create_session()` function is of particular interest, as shown below.

```
; int __cdecl create_session(char *dest, int)
public create_session
create_session proc near

    path= byte ptr -87Dh
    var_46C= dword ptr -46Ch
    s= byte ptr -414h
    var_10= dword ptr -10h
    var_8= dword ptr -8
    dest= dword ptr 8
    arg_4= dword ptr 0Ch

    push    ebp
    mov     ebp, esp
    push    ebx
    sub     esp, 894h
    call    sub_2AB7
    add     ebx, 3DAFh
    lea     eax, [ebp+s]
    mov     edx, eax
    mov     eax, 400h
    mov     [esp+8], eax    ; n
    mov     dword ptr [esp+4], 0 ; c
    mov     [esp], edx     ; s
    call    _memset
    call    _get_curttime
    mov     [ebp+var_8], eax
    mov     dword ptr [esp], 0 ; timer
    call    _time
    mov     [esp], eax     ; seed
```

.net (1) Oday (4) **Odays**  
(11) **advisory** (6) alcatel  
(1) avant browser (3) beef (2)  
bookmark (1) brute force pin  
callmanager cisco phone (1) burp  
(2) burp extension (1) burp pro  
(2) burpcsj (3) corba (1) cors (1)  
crash (1) **crawljax** (3) **csrf** (2)  
CVE-2016-2246 (1) cve2015-2526  
(1) cve2016-3374 (1) dos (1) edge  
(1) **exploit** (5) feed (1) file  
upload (1) firefox (1) giop (1)  
hitb2012ams (2) hitb2017ams (1)  
hp (2) html5 (1) i.maxthon.com (1)  
integer overflow (1) **junit** (3)  
kemp (1) kiosk hacking (2) load  
master (1) lucent (1) **maxthon**  
(5) mcafee (1) **metasploit** (2)  
microsoft (1) ms16-115 (1) mvc (1)  
omniorb (1) omnivista (1) oracle  
**glassfish** (2) pdf (1) **poc** (4) rce  
(1) redos (1) regex (1) remote  
code execution (2) root shell  
(2) **security** (2) **security**  
conference (2) **selenium** (3)  
selenium ide (1) smex (1) **sop** (2)  
thinpro (2) trend micro (1)  
trendmicro (2) tutorial (1)  
unauthenticated (1) uxss (1) **web**  
**application testing** (4) **web**  
**hacking** (3) **xcs** (4) xhr (1) xsrf  
(1) **xss** (3) zero client (1)

## Blog Archive

▼ **2017** (2)

```

mov     [esp], eax      ; seed
call    _srand
call    _rand
mov     [ebp+var_10], eax
mov     eax, [ebp+var_10]
mov     [esp+0Ch], eax
lea     eax, (a1 - 8298h)[ebx] ; "%i"
mov     [esp+8], eax    ; format
mov     dword ptr [esp+4], 400h ; maxlen
mov     eax, [ebp+dest]
mov     [esp], eax      ; s
call    _snprintf
mov     eax, [ebp+dest]
mov     [esp], eax      ; dest
call    _do_md5
mov     eax, [ebp+arg_4]
mov     edx, [eax+28h]
lea     eax, [ebp+s]
mov     [esp+8], eax    ; char *
mov     [esp+4], edx    ; int
mov     eax, [ebp+dest]
mov     [esp], eax      ; int
call    _get_session_ID

```

This function performs the following actions:

- Gets current time
- Use time as "seed"
- Use srand() with above seed
- MD5 hash the rest

All these functions can be shortened as the following: `session_id = md5(srand(get_curtime()))`

The vulnerability is that the seed is predictable, and therefore an attacker can generate session IDs issued in the past.

However, there are two conditions which affect exploitation of this vulnerability:

▼ April (2)

UXSS in  
McAfee  
Endpoint  
Security,  
[www.mcafee.com](http://www.mcafee.com) a...

Trend Micro  
Threat  
Discovery  
Appliance -  
Session G...

► 2016 (4)

► 2015 (3)

► 2014 (1)

► 2013 (3)

► 2012 (13)

► 2011 (2)

#### Old site - Last 5 Articles

UXSS in McAfee Endpoint  
Security, [www.mcafee.com](http://www.mcafee.com)  
and some extra  
goodies... - 4/26/2017

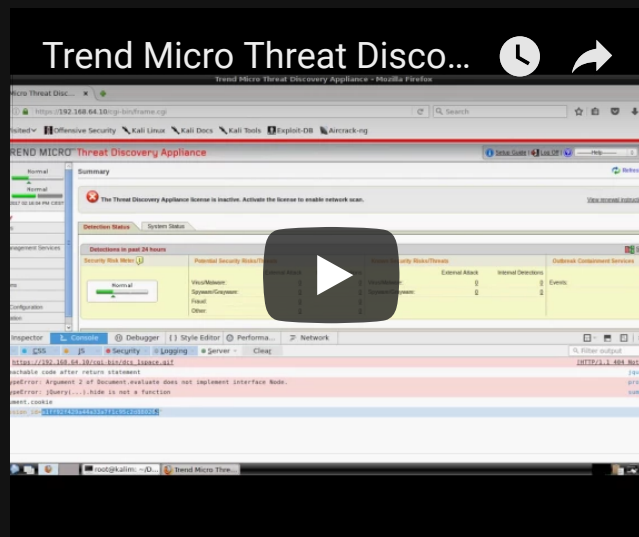
Trend Micro Threat  
Discovery Appliance -  
Session Generation  
Authentication Bypass  
(CVE-2016-  
8584) - 4/20/2017

- 1) A legitimate user has to be authenticated - a session token is associated with an IP address when a user logs in
- 2) Attacker needs to perform the attack with the same IP address of legitimate user

The second condition is not an issue in a NATed environment but in a different environment it's definitely the most significant constraint.

A further conclusion is that although the attacker is able to technically predict "future" session\_id tokens, there is no point in doing that, since condition (1) has to be met first and an association between an IP address and session\_id has to exist in the database.

The exploit Proof-of-Concept (poc) has been published [here](#) and below a video showing the attack in action:



The exploits for all the other TDA vulnerabilities that were discovered as part of this research can be found below:

[CVE-2016-8584](#) - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 (latest) Session Generation Authentication Bypass Vulnerability

[CVE-2016-7547](#) - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 dlp\_policy\_upload.cgi Information Disclosure Vulnerability

[Alcatel Lucent Omnivista or: How I learned GIOP and gained Unauthenticated Remote Code Execution \(CVE-2016-9796\)](#) - 12/1/2016

[Pwning a thin client in less than one minute, again!](#) - 10/3/2016

[Microsoft Windows PDF Library Information Disclosure Vulnerability - CVE-2016-3374 \(MS16-115\)](#) - 9/14/2016

Subscribe To

 Posts

 Comments

CVE-2016-7552 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 logoff.cgi Directory Traversal Authentication Bypass Vulnerability

CVE-2016-8585 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 admin\_sys\_time.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8586 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 detected\_potential\_files.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8587 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 dlp\_policy\_upload.cgi Remote Code Execution Vulnerability

CVE-2016-8588 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 hotfix\_upload.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8589 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 log\_query\_dae.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8590 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 log\_query\_dlp.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8591 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 (latest) log\_query.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8592 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 (latest) log\_query\_system.cgi Command Injection Remote Code Execution Vulnerability

CVE-2016-8593 - Trend Micro Threat Discovery Appliance <= 2.6.1062r1 (latest) upload.cgi Remote Code Execution Vulnerability

A Metasploit module has been developed and added to the master branch:

[https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/trendmicro\\_threat\\_discovery\\_admin\\_sys\\_time\\_cmdi.rb](https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/http/trendmicro_threat_discovery_admin_sys_time_cmdi.rb)



Posted by [Roberto Suggi Liverani](#) at [09:59:00](#)



Labels: [Oday](#), [exploit](#), [hitb2017ams](#), [trend micro](#), [trendmicro](#)

## 2 comments:



**Anonymous** [22 April 2017 at 16:12](#)

That product is no longer relvent and is no longer sold

[Reply](#)



**Roberto Suggi Liverani**  [26 April 2017 at 13:38](#)

Yes, product is EOL (End Of Life), as stated in the slides of the presentation as well. A further reason to disclose associated vulnerabilities.

[Reply](#)

Enter your comment...



Comment as:

Google Accoun ▼

**Publish**

Preview

[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)