Nmap Security Scanner
- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists
- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools
- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News
Advertising
About/Contact

Site Search

Sponsors:

FULL DISCLOSURE Full Disclosure mailing list archives

By Date By Thread

Google™ Custom Search Search

Trend Micro Direct Pass - Filter Bypass & Persistent Web Vulnerability

From: Vulnerability Lab <research () vulnerability-lab com>
Date: Thu, 28 Jan 2016 15:00:12 +0100

```
Document Title:
===============
Trend Micro Direct Pass - Filter Bypass & Persistent Web Vulnerability


References (Source):
====================
http://www.vulnerability-lab.com/get_content.php?id=1661

Video: http://www.vulnerability-lab.com/get_content.php?id=1688


Release Date:
=============
2016-01-28


Vulnerability Laboratory ID (VL-ID):
====================================
1661


Common Vulnerability Scoring System:
====================================
6.6


Product & Service Introduction:
===============================
DirectPass runs as a local console and browser plug-in but can also sync between multiple PC installations through you
Trend Micro account.
Unlike LastPass 1.72 (free, 5 stars), Dashlane (free, 4.5 stars), and RoboForm Everywhere 7 ($19.95 direct, 4.5 stars)
it doesn`t let you
log in to your saved credentials online. However, it will sync with free DirectPass apps for Android and iPhone. You
can also test a free
edition that manages just five passwords.

DirectPass can export its data for import to another DirectPass installation. It can also import login data from
LastPass. Hoping to get a
fast start, I imported my 200+ LastPass logins. The results were disappointing. For starters, DirectPass doesn`t
include the ability to
categorize sites, so my passwords came through as an unordered list, a very long list. There`s no way to sort the list
and no provision to
search for a particular login. For some reason, clicking in the list`s scroll bar doesn`t scroll down by one  `page` o
items. Instead, it
scrolls to the corresponding location in the list. Finding any particular login required tediously scrolling through
the entire list.

(Copy of the Vendor Homepage: https://www.directpass.com/signin )


Abstract Advisory Information:
==============================
An independent vulnerability laboratory researcher discovered a filter bypass and persistent vulnerability in the
official Trend Micro DirectPass web-application.


Vulnerability Disclosure Timeline:
==================================
2016-01-16: Researcher Notification & Coordination (Benjamin Kunz Mejri - Evolution Security GmbH)
2016-01-17: Vendor Notification (Trend Micro Security Team)
2016-01-18: Vendor Response/Feedback (Trend Micro Security Team)
2016-01-21: Vendor Fix/Patch (Trend Micro Developer Team)
2016-01-27: Security Bulletin (Trend Micro Security Team) [Acknowledgements]
2016-01-28: Public Disclosure (Vulnerability Laboratory)


Discovery Status:
=================
Published


Affected Product(s):
```

```
====================
Trend Micro
Product: DirectPass 2016 Q1


Exploitation Technique:
=======================
Remote


Severity Level:
===============
High


Technical Details & Description:
================================
A filter bypass issue and corss site request forgery web vulnerability has been discovered in the official Trend Micro
Direct Pass web-application.
The vulnerability allows remote attackers to bypass the input filter to inject own malicious script codes to the
application-side of the online-service.

This persistent vulnerability allows an attacker to execute javascript inside the password hint box! This would allow
an attacker to trick a victim to logging
into an account and then when the victim inserts a wrong master-password, a malicious javascript payload executes. The
vulnerability is located on the
application-side and the request method to inject is POST. The validation of the input is wrong encoded and suffers
from a persistent vulnerability.

The security risk of the filter bypass and persistent validation vulnerability is estimated as high with a cvss (commo
vulnerability scoring system) count of 6.1.
Exploitation of the persistent input validation web vulnerability requires a low privileged direct-pass user account
with restricted access and low or medium user interaction.
Successful exploitation of the vulnerability results in session hijacking, persistent phishing, persistent external
redirects to malicious source and persistent manipulation
of affected or connected application modules.

Vulnerable Module(s):
                                [+] Password Hint - Input Box

Affected Module(s):
                                [+] Direct Pass - Web Application


Proof of Concept (PoC):
=======================
The vulnerability can be exploited by remote attackers with low privileged web-application user account and low user
interaction.
For security demonstration or to reproduce the vulnerability follow the provided information and steps below to
continue.

Manual steps to reproduce the vulnerability ...
1.  Go to https://www.directpass.com and sign-in
2.  Go to https://www.directpass.com/showdb#settings/master
3.  Change your master password
4.  Then insert your master password
5.  Then insert the new master password and confirm master password
6.  For the Hint, right-click on the box and click inspect element and remove maxlength="20" from the code
7.  Then put ur XSS payload into the Hint box!
8.  Logout from your account
9.  Login to your account
10. Insert your master-password wrong and your  XSS payload executes!
Note: This vulnerability also effects the beta/duplicated version of the website: http://pwm-ibeta.trendmicro.com

PoC Video: https://www.youtube.com/watch?v=vXCdjK6O-Pc


Solution - Fix & Patch:
=======================
The vulnerability can be patched by a secure parse and encode of the vulnerable password hint input.
Disallow special chars and restrict the input via filter exception.


Security Risk:
==============
The security risk of the input validation web vulnerability and filter bypass  in the direct-pass web-application of
trend micro is estimated as high. (CVSS 6.6)


Credits & Authors:
==================
Karim Rahal [Karim () karimrahal com / KarimMTV () elitesec org] - @KarimMTV
[http://www.vulnerability-lab.com/show.php?user=Karim%20Rahal]


Disclaimer & Information:
=========================
The information provided in this advisory is provided as it is without any warranty. Vulnerability Lab disclaims all
warranties, either expressed
or implied, including the warranties of merchantability and capability for a particular purpose. Vulnerability-Lab or
its suppliers are not liable
in any case of damage, including direct, indirect, incidental, consequential loss of business profits or special
damages, even if Vulnerability-Lab
or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or
```

limitation of liability for
consequential or incidental damages so the foregoing limitation may not apply. We do not approve or encourage anybody to break any vendor licenses,
policies, deface websites, hack into databases or trade with fraud/stolen material.

```
Domains:    www.vulnerability-lab.com          - www.vuln-lab.com                                     - www.evolution-sec.com
Contact:    admin () vulnerability-lab com     - research () vulnerability-lab com                    - admin () evolution-sec com
Section:    magazine.vulnerability-db.com      - vulnerability-lab.com/contact.php                    - evolution-sec.com/contact
Social:     twitter.com/#!/vuln_lab            - facebook.com/VulnerabilityLab                        - youtube.com/user/vulnerability0lab
Feeds:      vulnerability-lab.com/rss/rss.php  - vulnerability-lab.com/rss/rss_upcoming.php           - vulnerability-lab.com/rss/rss_news.php
Programs:   vulnerability-lab.com/submit.php   - vulnerability-lab.com/list-of-bug-bounty-programs.php - vulnerability-lab.com/register/
```

Any modified copy or reproduction, including partially usages, of this file requires authorization from Vulnerability Laboratory. Permission to
electronically redistribute this alert in its unmodified form is granted. All other rights, including the use of other media, are reserved by
Vulnerability-Lab Research Team or its suppliers. All pictures, texts, advisories, source code, videos and other information on this website
is trademark of vulnerability-lab team & the specific authors or managers. To record, list (feed), modify, use or edit our material contact
(admin () vulnerability-lab com or research () vulnerability-lab com) to get a permission.

--
VULNERABILITY LABORATORY - RESEARCH TEAM
SERVICE: www.vulnerability-lab.com
CONTACT: research () vulnerability-lab com
PGP KEY: http://www.vulnerability-lab.com/keys/admin () vulnerability-lab com%280x198E9928%29.txt

By Date   By Thread

Current thread:

- Trend Micro Direct Pass - Filter Bypass & Persistent Web Vulnerability *Vulnerability Lab (Jan 28)*

[Nmap | Sec Tools | Mailing Lists | Site News | About/Contact | Advertising | Privacy]
Google™ Custom Search Search