Advisory

# Gmail - Google Docs Cookie Hijacking through PDF Repurposing Attack



Aditya K Sood, (C) SecNiche Security Email: adi\_ks [at] secniche.org

## Disclaimer

2009 All Rights Reserved. SecNiche makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of SecNiche. While every precaution has been taken in the preparation of this publication, this publication and features described herein are subject to change without notice

## Responsible Disclosure

May 5 2009 –
Responsible Disclosed to Google Security Team
May 5 2009 –
Google started investigation of the vulnerability.
May 6 2009 –
Proof of Concept was shared with Google Security Team
May 7 2009 –
Google reproduced the issue and started working on it.
May 8 2009 –
A non disclosure notification was sent as per Google requirement
May 9 2009 –
Google deployed the requisite recommendation.
May 11 2009 –
Advisory Released

# Points to Consider:

- [1] The whole network of Google docs has been changed and there will be no use of Adobe Acrobat Plugin.
- [2] The custom designed application should avoid using acrobat plugin in opening PDF documents.
- [3] Number of applications are still vulnerable to these type of inherent attacks.

#### Discussion:

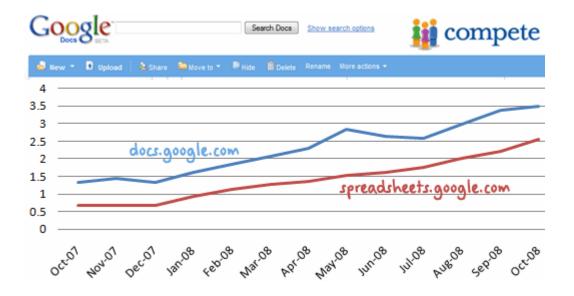
This attack depends on Adobe plugin used in browsers for opening of PDF files. There is another modified approach to trigger web attacks through JavaScript protocol handler in the context of browser when a PDF is opened in it. As we have seen, the kind of security mechanism implemented by Adobe in order to remove the insecurities that originate directly from the standalone PDF document in order to circumvent cross domain access. The attack is targeted on the web applications that allow PDF documents to be uploaded on the web server. Due to ingrained security mechanism in PDF Reader, it is hard to launch certain attacks. But with this technique an attacker can steal generic information from website by executing the code directly in the context of the domain where it is uploaded. The attack surface can be diversified by randomizing the attack vector. On further analysis it has been observed that it is possible to trigger phishing attacks too. Successful attacks have been conducted on number of web applications mainly to extract information based on DOM objects. The paper exposes a differential behavior of Acro JS and Brower JavaScript. More details on this type of attack can be seen here:

## **Detailed Paper**

## http://secniche.org/papers/SNS\_09\_03\_PDF\_Silent\_Form\_Re\_Purp\_Attack.pdf

This attack can be used to hijack Gmail/ Google doc cookies efficiently if certain conditions are met. The Google docs are an integrated service provided by Google for online viewing the document. A user logged in to Gmail will have the same cookie used for if any document. The interdependency can be exploited through this attack vector.

According to Compete, Google Docs had around 4.4 million unique visitors in September with docs.google.com attracting nearly twice as many unique users as spreadsheets.google.com on average



Last year stats about usage of Google Docs

#### The attack can be structured as:

1. An Attacker sends a well crafted PDF file to victim containing the execution code.

2. Victim opens the file in the default PDF Viewer by Google. There is a proper conversion take place and document is converted into different format so that no intermediate DOM calls can be executed. The Google has done a good work in this by keeping the human interaction to minimum.

3. If a victim chooses to open that PDF file directly from Google PDF viewer for print, the attack is successful. This is because the PDF during print process is converted back into original format and opened in the browser. So there is no differential check is present and PDF becomes as a active and dynamic content having an appropriate interface with the browser. So now it is possible to extract cookies from it.

The attack is successfully triggered in number of situations and cookie can be extracted easily while user is logged into his/her account. The problem that favors this attack in concern to Gmail is the rendering of PDF directly into browser which should not be allowed.

We will demonstrate this attack with appropriate steps as under mentioned:

### Step 1: An attacker sends an Email with malicious PDF as an attachment.



pdf_silent_http_form_check.p Downlead.(4820) Print.(1.page) Plain			Powered	by Google Docs
	[	PDF Silent HTTP Form Repurposing Attacks JavaScript DOM Call Execution Attack Vector - Pen Testing Web Application : PDF Uploading (Open it in Web Browser - Not Designed for Stand Alone PDF's) Addys & Soci , Founder Sectificity Security Definite Cift for You on your Birthday - My Dear (Coskie) Definite Hug for You on your Birthday - My Dear (Coskie) ton : Whether JavaScript protocol Handler is allowed. The Reason Acros 35 does not support D calls where as Browser based JavaScript does.	OM	

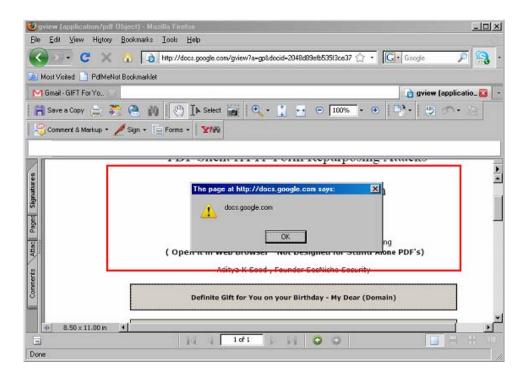
# Step 2: Victim opens the PDF directly in the Google Doc viewer.

# Step 3: Victim tries to print the document directly from viewer.

Ble	Edit View Higtory Bookmarks Icols Help	0	
<	💽 🔹 🗶 🧄 Mpc//docs.google.com/gwiew?a-golido 😭 🔹 🖾 🕻 Google	Print	2 🛛
M	Host Visited 📑 PdMeNat Bookmaklet	Printer	
	Gnul - BITT For	Name: Adobe PDF	Properties
6	i 🚍 🎘 🤮 🙌 🕐 🕽 Seet 📷 🔍 - 👔 🖻 🤉 226 - 😐	Status: Ready Type: Adobe PDF Converter	Conments and Forms: Document and Stamps
18	🖉 🔹 🕞 🛛 😓 Connert & Heriup + 🥖 Sign + 📄 Forms + 🛛 🏋 🕅	Print Range Ø All	Parview 8.5
		C Current view	Ť
50		C Constronge C Pagestion 1 to 1	2017 Administrative Tara Representative Administrative Developing 2016/2018 Research
Signatures	PDF Silent HTTP Form Repurposing Attacks	Subset All pages in range 🔄 🗖 Flevence pages	VALUES AND ADDRESS
Pages 1	JavaScript DOM Call Execution	Page Handing Copies: 1 🚆 🗖 Define	
<u>د</u>		Page Scaling: Reduce to Printer Margine	EG STATE OF STATE OF STATE
	Attack Vector - Pen Tecting Velo Application - POF Uploading ( Open it in Web Browser - Not Decigned for Stand Alone PDF K)	P Auto-Rotate and Center	
100	Aditys K Sood , Pounder SedNiche Security	Choose Paper Source by PDF page size	
Attechnento	Definite Gift for Tox on your Birthday - Hy Doar (Demain)	T Pint to life	
7	Definite Reg for Yes on your Birthday - My Dear (Ceshie)	F Print color at black	Units: Inches Zoom: 100%
Connecto	Contractions : whether assaulting protocol wandler is allowed. The vasion words as doet not exppo- calls where as Browser based JavaScript does.		
8	Another way to perform Penetration testing of Web Applications. This is extensively used only malicicus PDF's are allowed to be reposed on the web server. When registed PDF file is opene- Biowere 7.8 anachies DDM Calls	Printing Tips Advanced	OK Cancel
	Worked Efficiently with		
Dor			

Once the PDF is opened in the browser it depends on the attacker the way he has designed the PDF. In our POC a form has been designed which worked as mentioned below:

# [3.1] Gmail/Google Doc - Domain Check



# [3.2] Gmail/Google Doc - Cookie Extracted

Ele Édit Ýjew Higtory Bookmarks Loois Help   Image: State of the state of
🕜 🖂 😋 🗶 🍙 http://docs.google.com/gview?a=gp&docid=2048d33elb53513ce37 🏠 🔹 💽 • Google 🔎 🤮
🔎 Most Visited 📋 PdiMeNot Bookmarklet
M Gmail - GIFT For Yo 🗵
📔 Save a Copy 🚖 🚔 🤮 🙌 🔯 🕐 🚺 Select 📷 🔍 - 📜 🔤 🗢 100% - 💿 📑 - 😢
Comment & Markup - 🖉 Stan - 🚍 Forms - 🏼 🏹 🕅
The page at http://docs.google.com says:
SID=DQAAAHwaAAAKRiixiddwiBrXZ2MEMkoUEyVvkkPBIwukuLg1s0Dv7tKuLaMy3EjväLoLaL_dMHLioSDI415wFx2V470QJN2E5MRqtNpEbOR5y- JDN0gXoZELEQtanqHExkP6S04A2Hy9ELvgQsQL7oqpmSOLDPbC7NysrcE8g35g; WRITELY_SID=DQAAAIAAACVVCCGuHKINOBKcMVxTR2bma3XT_DBPQNLFUBBIZJqcs55uwlTM5yYOI2YR- JISWBWnLhDdTmVQ3bYMqk77WEMMmuDNANNzUqS4nHmobzTgTUHK30ZiAhnitQUYzay5gbtMeht2g596rq24oov3J0pSZW76p5BSLFiCagg OK
Definite Gift for You on your Birthday - My Dear (Domain)
Definite Hug for You on your Birthday - My Dear (Cookie)
8
Contradiction : Whether JavaScript protocol Handler is allowed. The Reason Acros JS does not support DOM calls where as Browser based JavaScript does.

The page at http://docs.google.com says:	
PREF=ID=b58019ebb96bd8f8:U=eb85e4a0863d5842:TM=1240839881:LM=1241117976:DV=AA:GM=1:IG=1:S=BdswFl0xUl4vwtvJ; TZ=-330; S=photos_html=APfhCHaJZT:pDRasiiq33g:indic-transliteration=SduMpmVb4_Luz2ov/1edC0g; SID=DQAAAHwAAAAKRisxd4dvlbRxZZMEMitsUEJVvkKPBIwu4mLg1s00XTKMLslAMy3EjvzLoLaL_dxMhLicS01415xrFx2V470QJN2E5t4RqtfNpEb0R5y JDN0gXo0ZEL6QtanqHExkP6504A2Hyy8ELvgQsQL7oqpmiS0LDPbC7NySrrcE6g3Sg; WRITELY_SID=DQAAAIAAAACWXCGuhHKJN08kcMXur7bR2bma3XT_DBPQNLIFUb8JZJqcs55uwlTiM5yY0I2YR- JfSWBWnLhDdTmVQ3bYMqk77WEMMmuDNANNzUqS4nHmobzTgTUHh3DZiAhnrfQUYzay5gbrMeht2g596rqZ4oov3J0pSZW76p5IBSLFiCagg	-
ОК	

That's how the PDF Repurposing Attack can be triggered.