]HackingTeam[

RCS Exploit Package

Whitepaper

THIS DOCUMENTATION IS STRICTLY CONFIDENTIAL

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

Document Approval

Revision	Author(s)	Release Date
1.0		

Table Of Contents

1 Overview

The majority of software applications contain a certain number of defects that can be *exploited* to take control of the software itself in order to install unwanted applications.

Relying on those flaws, it’s possible to turn normal documents into installation vectors for RCS, adding a new way of starting investigations to the selection proposed by Hacking Team.

Hacking Team Exploits Package is accessed by the Remote Control System Console and allows to easy embed the agents into most of the common file formats: *Adobe Pdf*, *Microsoft PowerPoint* and *Word documents*, just to give a few examples.

Once opened on the target computers, the document carrying the exploit will install an RCS agent.

2 The Package

Exploits normally require a high skill level to be used, and that may not be readily available. Hacking Team combined its expertise in offensive security and software design to embed the exploits as installation vectors for RCS agents.

2.1 What is an exploit?

An exploit is a piece of code that can be injected into flawed software to take control of it.

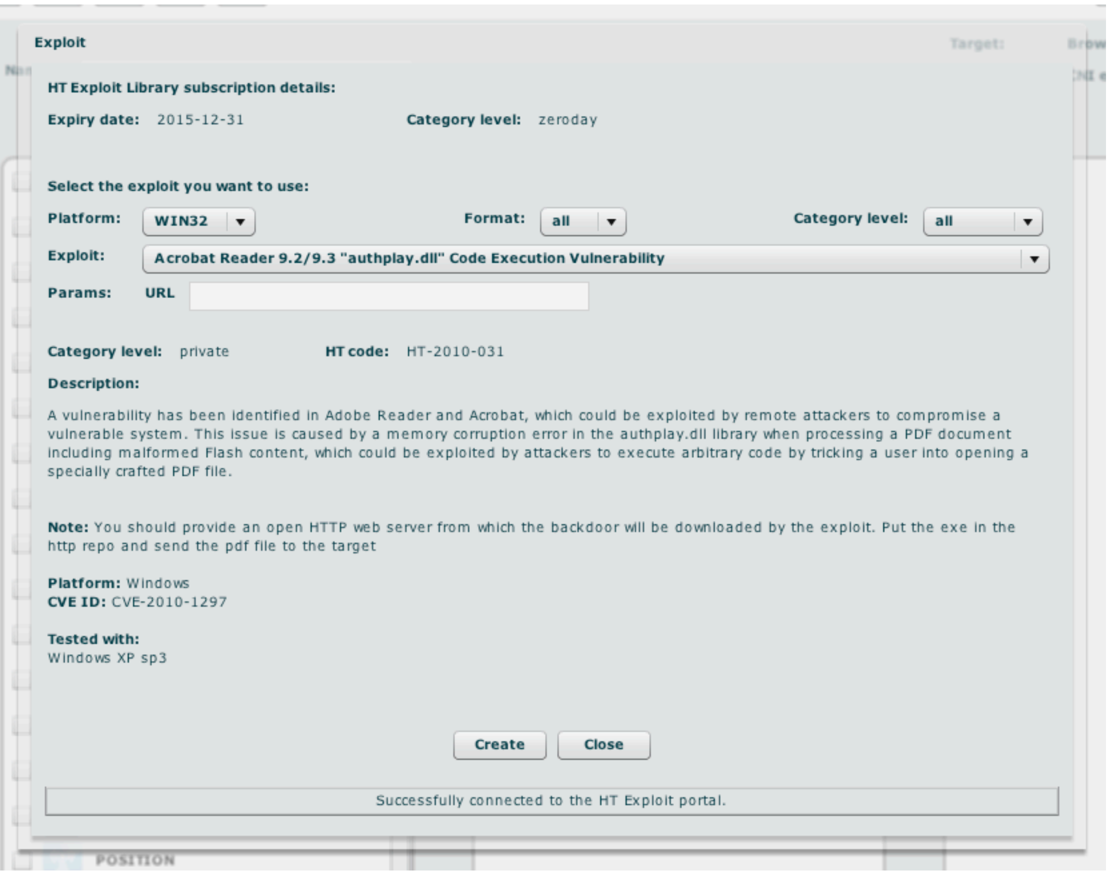
In the layman view, exploits are seen as black magic: some obscure piece of code written by hackers and usable only by them.

2.2 Why a Package?

Hacking Team, with the Exploit Package, took away all of the difficult part of using exploits and made them easy.

Hacking Team Exploit Package is a repository of client side exploits ready to be used.
Each exploit available is selected by Hacking Team to be effective against common application software, such as web browsers and office applications.

The exploit repository resides on the end-user server and can be easily accessed from within the RCS Console.



HT Exploit Library subscription details:

Expiry date: 2015-12-31 Category level: zeroday

Select the exploit you want to use:

Platform: WIN32 Format: all Category level: all

Exploit: Acrobat Reader 9.2/9.3 "authplay.dll" Code Execution Vulnerability

Params: URL

Category level: private HT code: HT-2010-031

Description:

A vulnerability has been identified in Adobe Reader and Acrobat, which could be exploited by remote attackers to compromise a vulnerable system. This issue is caused by a memory corruption error in the authplay.dll library when processing a PDF document including malformed Flash content, which could be exploited by attackers to execute arbitrary code by tricking a user into opening a specially crafted PDF file.

Note: You should provide an open HTTP web server from which the backdoor will be downloaded by the exploit. Put the exe in the http repo and send the pdf file to the target

Platform: Windows
CVE ID: CVE-2010-1297

Tested with:
Windows XP sp3

Successfully connected to the HT Exploit portal.

Each time an operator access the Exploit repository, the Console lists the available exploits and allows the creation of documents containing RCS agent.

2.3 Exploit Categories

Each of the available exploits is rated depending on a specific set of parameters.

RCS Exploit Package organizes exploits in categories, each one specifying a different availability level of the exploit, and the related software flaw, among application vendors and security experts.

As an example, for exploits categorized as public the software flaw they base upon are known, probably already patched and the raw exploits code is publicly available. This means that probably the effectiveness of this kind of exploit is not the best, but they still work and probably are still common among users of the flawed application.

Hacking Team organizes exploits in four categories:

Category	Description
Social	This category of exploits do not rely on specific software flaws, but on the user errors in using the documents. For example, a user opens an executable file believing it's a PDF document, since the original file extension is hidden by Windows.
Public	For public exploits, the software flaw is known and maybe it's also patched for the latest versions of the application. The exploit code is publicly available on the Internet.
Private	The exploit is built relies on a known vulnerability, but there is no publicly available exploit code. Vendors may have patched the flaw but no technical information is available, so writing an exploit is a difficult task.
Zero-day	The exploit is built relies on an unknown vulnerability, not even by the vendor of the application, thus no exploit code is available. These are the most powerful exploits since even the latest versions of the software are flawed.

This categorization permits you to have a wide selection of usable exploits all the time targeting different software. Moreover, depending on the specific scenario you're confronting with, you may want to preserve private or zero-day exploits as last resorts, and feel free to use social and public with less concern.

The availability of new “zero day” Exploits relies on the discovery of new vulnerabilities, thus new Exploits.

As soon as new “zero day” Exploits are found and/or purchased on the market, we will inform our clients with the list and the cost.