]HackingTeam[

RCS Exploit Portal

Whitepaper

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
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

Every software application contains a discrete number of security holes (aka *vulnerabilities*) that can be *exploited* to take control of the software itself in order to install unwanted applications.

Relying on those security holes, it’s possible to turn normal documents into installation vectors for RCS.

HackingTeam Exploit Portal, part of the Remote Control System platform, is a service that embeds an RCS Agents into common file formats, such as *Adobe PDF*, *Microsoft PowerPoint* and *Word documents*.

Installation of the RCS Agent is started as soon as the target opens the exploit document.

2 The Service

HackingTeam combined its expertise in offensive security and software design to build a service that make simple to prepare and use exploits as installation vectors for RCS agents.

2.1 What is an exploit?

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

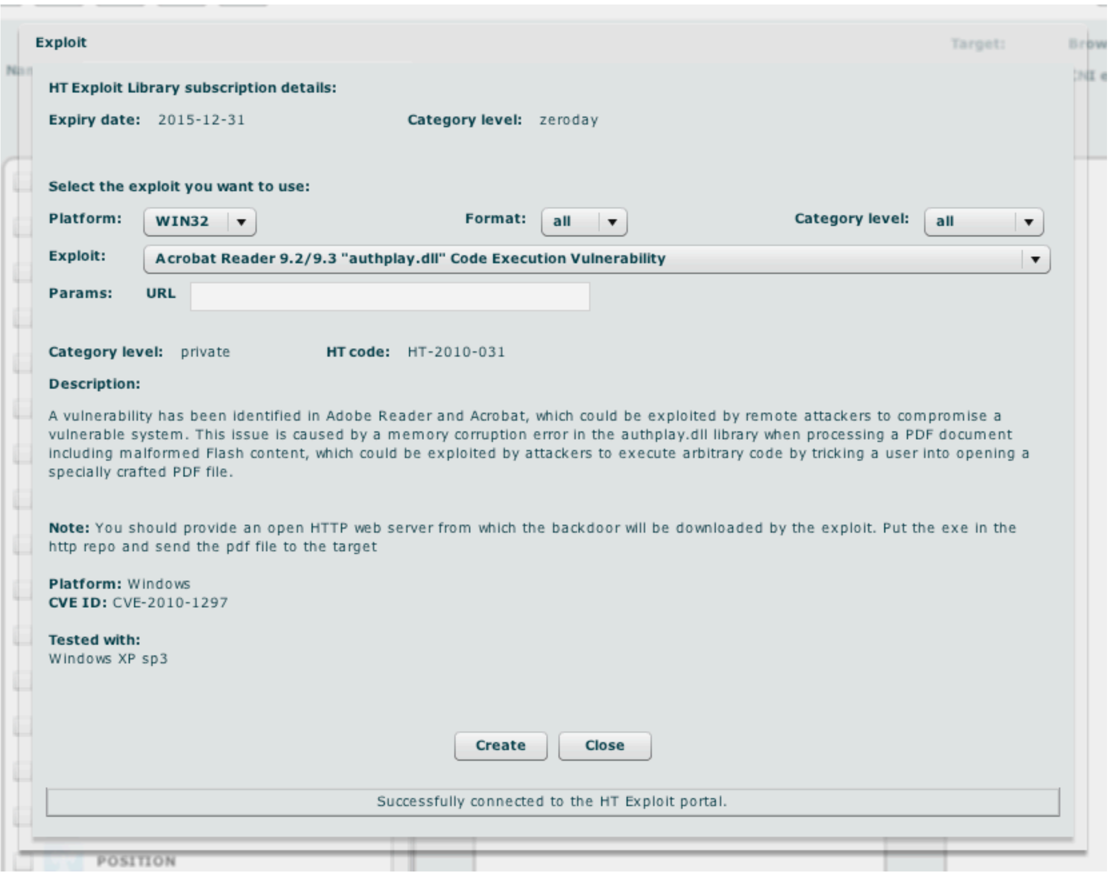
In the layman view, exploits are seen as part of an elite hacker toolkit: some obscure piece of code usable only by those who know the most obscure hacking techniques.

That was true since the introduction of the exploit portal, which made those techniques accessible even to untrained personnel.

2.2 Why a Portal?

HackingTeam Exploit Portal is a repository of client side exploits ready to be used.
Each exploit available was selected for its effectiveness against common application software, such as web browsers and office applications.

The exploit repository resides on HackingTeam servers, and it can be easily accessed from within the RCS Console.



Exploit

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 the operator access the Exploit Portal, the Console downloads the updated exploit list that allows for the creation of documents containing an RCS Agent.

NOTE Since exploits base their effectiveness upon software flaws, the list of available exploits may change at any time, therefore supported file formats may vary frequently.

2.3 Exploit Categories

Within the Exploit Portal exploits are organized in categories: each category specifies if whether the exploit is commonly available or exclusive to the Exploit Portal, and if the security hole it uses is publicly known or secret to everyone but HackingTeam.

As an example, for exploits categorized as *public*, the vulnerability they use is known and the raw exploit code is publicly available. This means that probably the effectiveness of this kind of exploit is not at its best, but they still work and probably the vulnerable application is still in wide use.

The exploit portal uses four categories to organize the available exploits:

Category	Description
Social	This category of exploits do not rely on security holes, but on errors made by the human target in opening the document. For example, an executable file can be concealed as a PDF by relying on the fact that Windows normally hides common file extensions: the target will see the usual file icon he's used to see on real PDF files, thus making him believe that it's safe to double click on it and open the document.
Public	For this category, the software flaw is known and the exploit code is publicly available on the Internet, tough the vulnerable version of the application is considered still widely adopted by a large user base.
Private	The exploit relies on a known vulnerability, but there is no public exploit code. No technical information is available on the vulnerability, so writing an exploit is a difficult task.
Zero-day	The exploit relies on a vulnerability not even known by the vendor of the application itself, and no exploit code is available. The latest version of the software is almost always vulnerable, thus making this exploit very effective even against users that update their installed applications frequently.

This categorization permits you to have a wide selection of usable exploits, targeting different applications and file formats. Therefore, depending on the specific scenario you're confronting with, you may want to preserve private or zero-day exploits as last resorts, first using the more expendable social and public exploits.

NOTE The Exploit Portal always contain at least three zero-day level exploits.