C2_Communication_of_ThreatNeedle.pdf

Sida 4 av 27

01. Server Analysis

An attacker could exploit this

vulerrability to execute arbitrary code on

the system with privileges of the victim.

ATMFD.dll in the Windows font library in

Microsoft Windows OS allows remote

attackers to execute arbitrary code via a

crafted web site.

CVE-2016-7256

IIS remote code execution vulnerability.

The ScStoragePathFromUrl function has

a buffer overflow vulnerability in the IIS

6.0 WebDAV service on Windows

Server 2003. The vulnerability allows an

attacker to run arbitrary code by

constructing a PROPFIND request with

a long header. So hackers can exsploit

the vulnerability by running code

remotely.

CVE-2017-7269

A webshell is a script written in the

supported language of a target web

server to be uplodaded to enable remote access and administration of the machine. The shell gives the creator the ability to crate, edit, download any file of choice, top of the list for infiltrators is using a web shell to gain root access to server.

Webshell
