

Advisory to Exploit

MS08-059

(Microsoft's Host Integration Server 2006)

#

MSF

Advisory to Exploit

➤ Who am I?

➤ Mario Ceballos < mc [a] metasploit.com >

➤ What do I do?

➤ Vulnerability Research / Exploit Development.

➤ metasploit framework developer.

➤ Focus is on auxiliary and exploit modules.

➤ What is this about?

➤ Process of exploiting one of the Microsoft Patch Tuesday vulnerability's.

The Bug

Remote exploitation of an arbitrary command execution vulnerability in Microsoft Corp.'s Host Integration Server 2006 could allow an attacker to execute arbitrary code with the privileges of the affected service.

The RPC interface exposes several methods that an unauthenticated attacker can use to execute arbitrary programs on the server. RPC opcodes 1 and 6 both allow an attacker to call the `CreateProcess()` function with full control over the application started, as well as the command line passed to it. This allows an attacker to run arbitrary programs on the server.

Vulnerability Highlights

- **Component for the remote management interface.**
 - **snarpcsv.exe**
- **RPC interface listens on a dynamic port.**
- **Universally Unique Identifier (UUID).**
 - **'ed6ee250-e0d1-11cf-925a-00aa00c006c1'**
- **RPC interface exposes 10 methods**
 - **rpc opcodes 1-6 allow unauthorized use of CreateProcess()**

Exploit Details

➤ **Open up snarpcsv.exe in IDA Pro.**

➤ **Run tenable's awesome mIDA plugin.**

```
/* opcode: 0x01, address: 0x01002CBB */
```

```
small _SnaRpcService_RunExecutable (  
    [in][string] char arg_1,  
    [in][string] char arg_2  
);
```

➤ **Also found that the interface is reached via.**

➤ **1.0/1.1 (version)**

➤ **ncacn_ip_tcp(endpoint protocol)**

➤ **tcp port is random, but we got that covered.**

MSF Module Details

- **No pointers involved, so it's in a auxiliary format.**
- **Makes use of the DCERPC exploit mixin.**
- **Automagically discover the tcp port via the endpoint mapper.**
- **Set your ARGS variable and shoot!**
 - **Default is '/c echo metasploit >metasploit.txt' ;)**

DEMO

#

MSF

References

- <http://www.metasploit.com>
- <http://cgi.tenablesecurity.com/tenable/mida.php>
- <http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=745>
- <http://www.microsoft.com/technet/security/bulletin/ms08-059.mspx>

Thanks!

Questions?

#

MSF