

OST
Ostschweizer
Fachhochschule

Bind, Reverse, Web-Shells

Einführung

Ivan Bütler

Abteilung Informatik, Rapperswil

Remote Code Execution (RCE)

- Ability to trigger arbitrary code execution over a network.
- This is the holy grail an attacker wants on your system!

CVE Details
The ultimate security vulnerability datasource

Search: Search
View CVE

[Log In](#) [Register](#)

[Home](#)
Browse :
[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)
Reports :
[CVSS Score Report](#)
[CVSS Score Distribution](#)
Search :
[Vendor Search](#)
[Product Search](#)
[Version Search](#)
[Vulnerability Search](#)
[By Microsoft References](#)
Top 50 :
[Vendors](#)
[Vendor Cvss Scores](#)
[Products](#)
[Product Cvss Scores](#)
[Versions](#)
Other :
[Microsoft Bulletins](#)
[Bugtraq Entries](#)
[CVE Definitions](#)
[About & Contact](#)
[Feedback](#)
[CVE Help](#)
[FAQ](#)
[Articles](#)
External Links :

Vulnerability Details : CVE-2017-0143 (6 Metasploit modules)

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
Publish Date : 2017-03-16 Last Update Date : 2018-06-20

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

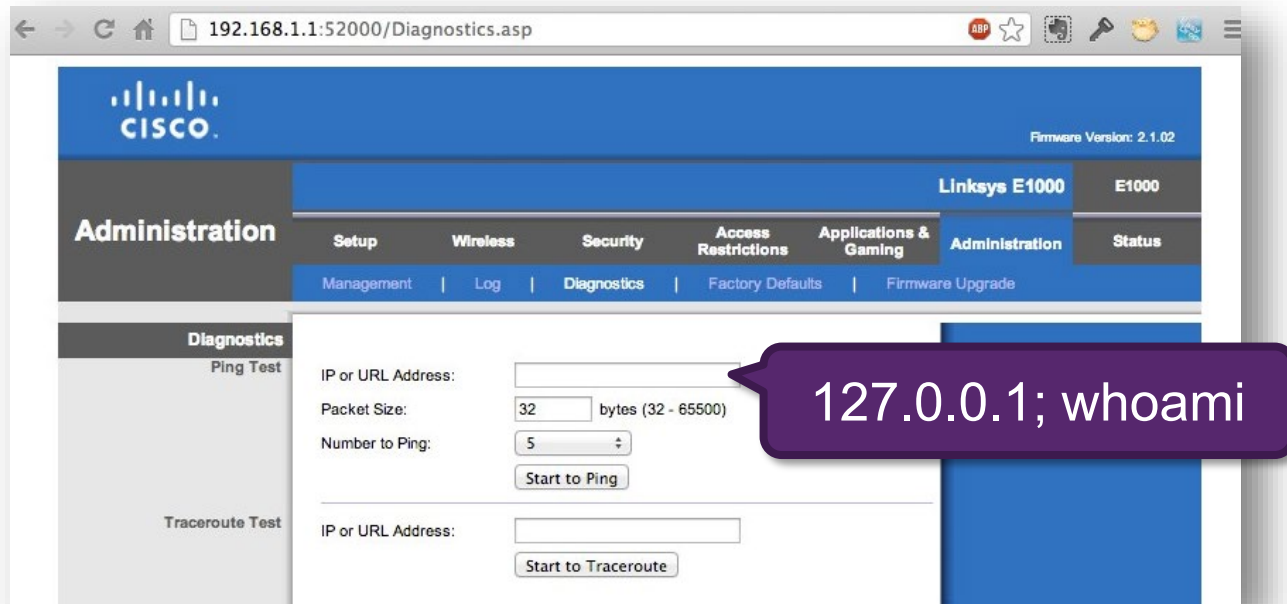
Products Affected By CVE-2017-0143

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Microsoft	Server Message Block	1.0				Version Details Vulnerabilities

Example of the
Eternalblue
Vulnerability

How to get RCE?

- Command Injection
- File Upload (Upload a PHP file to a webserver)
- SQL Injections can sometimes be used to get RCE
- Buffer Overflow (write own instructions into the process memory and execute it)
- ...



Exploit Limitation

- Often, an exploit can only execute one command at a time
- Shells can be used to interactively execute commands on the system
- There are multiple types of shells
 - Web Shells
 - Bind Shells
 - Reverse Shells



Web Shell



Upload Web Shell to Webserver on port 443

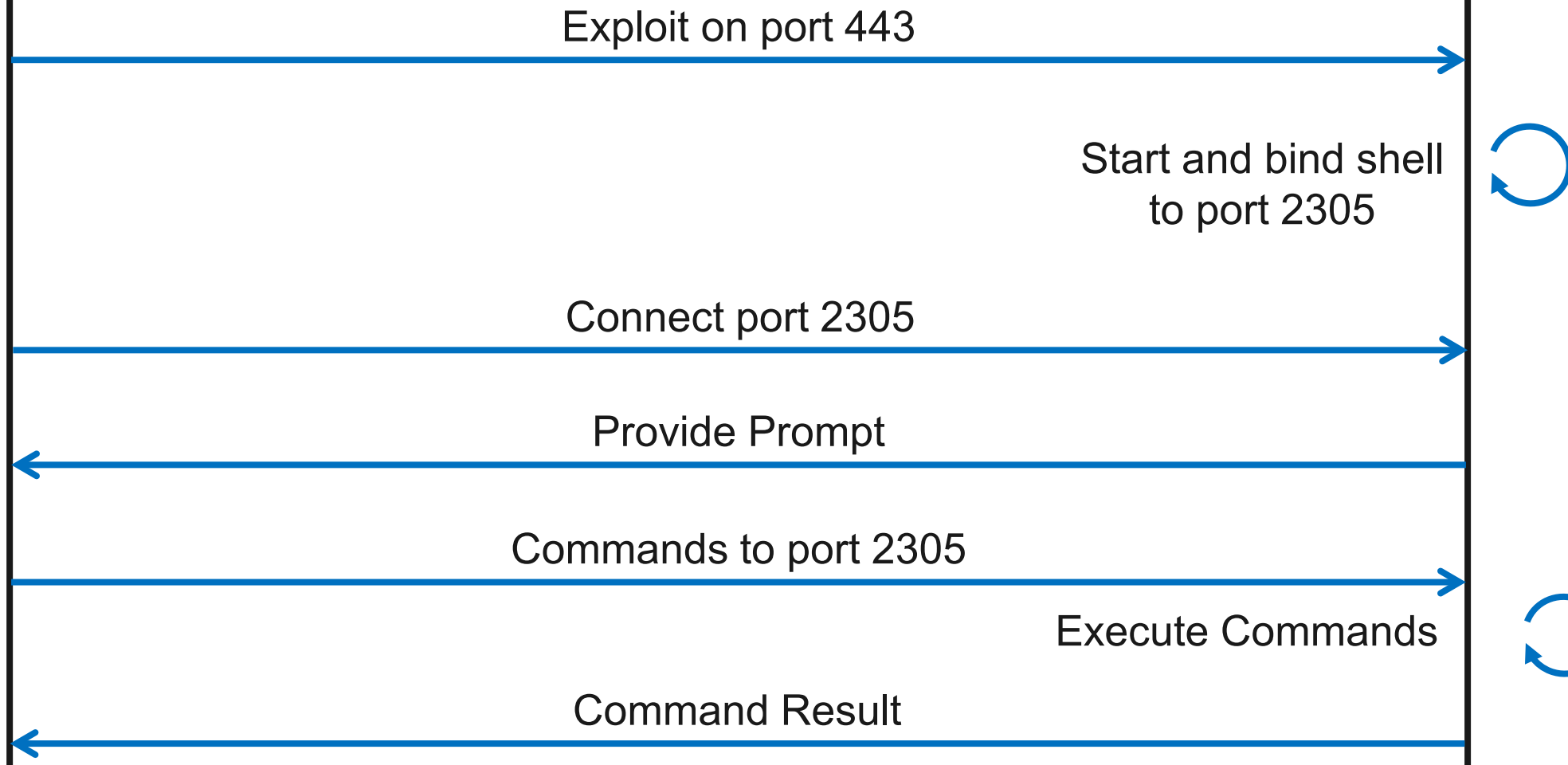
HTTP GET /shell.php?cmd=whoami on port 443

Execute Command

HTTP 200 OK, root



Bind Shell



Reverse Shell

