



## Win-2008 Assignment

---

Report generated by Nessus™

Wed, 15 Mar 2023 14:24:33 Singapore Standard Time

---

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.15.135.....	4
-----------------------	---

Nessus Essentials

---

## **Vulnerabilities by Host**

---

---

**192.168.15.135**



---

#### Scan Information

Start time: Wed Mar 15 14:16:31 2023  
End time: Wed Mar 15 14:24:32 2023

---

#### Host Information

Netbios Name: WIN-2008  
IP: 192.168.15.135  
MAC Address: 00:0C:29:22:E4:DE 00:0C:29:22:E4:D4  
OS: Microsoft Windows Server 2008 Enterprise Service Pack 1

---

#### Vulnerabilities

**35361 - MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)**

---

#### Synopsis

It may be possible to execute arbitrary code on the remote host due to a flaw in SMB.

---

#### Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

---

#### See Also

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2009/ms09-001>  
<https://www.zerodayinitiative.com/advisories/ZDI-09-001/>  
<https://www.zerodayinitiative.com/advisories/ZDI-09-002/>

---

#### Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

---

#### Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	31179
BID	33121
BID	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
MSKB	958687
XREF	MSFT:MS09-001
XREF	EDB-ID:6463
XREF	CWE:94
XREF	CWE:119
XREF	CWE:399

Exploitable With

Core Impact (true)

Plugin Information

Published: 2009/01/13, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

```
KB : 958687
- C:\Windows\system32\drivers\Srv.sys has not been patched.
  Remote version : 6.0.6001.18000
  Should be      : 6.0.6001.18185
```