

[Windows] Windows 랜섬웨어 & SMB 취약점 포트 차단

[Windows] Windows 랜섬웨어 & SMB 취약점 포트 차단

SMB

네트워크에 연결된 컴퓨터끼리 파일, 프린터, 포트 또는 기타 메시지를 전달하는데 사용된다.

SMB 프로토콜 원격코드 실행 취약점은 랜섬웨어 공격으로 많이 사용되고 있다.

OS 최신 보안 패치

MS에서 SMB 관련 취약점에 대한 패치는 보안 업데이트로 제공된다.
업데이트가 어려운 서버는 아래 SMB 포트 차단으로 조치 가능하다.

SMB 포트 차단

Powershell ISE에서 아래 내용 복사 후 실행
updated by Hostway System Team

```
$Language = Get-WinUserLanguageList  
$Lang = $Language.LanguageTag
```

```
Switch($Lang)
```

```
{  
    'ko'
```

```
{  
    Write 'OS Version'
```

```
[Environment]::OSVersion
```

```
Write-Verbose -Message "취약점 포트 제거 UDP 137, UDP 138, TCP  
139, TCP 445" -Verbose
```

```
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
```

```
In)" profile=public dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
In)" profile=private dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
In)" profile=public,domain dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
In)" profile=private,domain dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
In)" profile=private,public dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-Name-
In)" profile=any dir=in localport=137 protocol=udp new
enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=public dir=in localport=137 protocol=udp new
enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=private dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Name-In)" profile=any dir=in localport=137 protocol=udp new
enable=no
```

```
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=public dir=in localport=137 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
```

```
Datagram-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=any dir=in localport=137 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=public dir=in localport=138 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=public,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=private,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=private,public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Datagram-In)" profile=any dir=in localport=138 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=public dir=in localport=138 protocol=udp
new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
```

```
Datagram-In)" profile=public,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=private,domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=private,public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="네트워크 검색(NB-
Datagram-In)" profile=any dir=in localport=138 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=public dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=private dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=public,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=private,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=private,public dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="가상 컴퓨터 모니터링(NB-
Session-In)" profile=any dir=in localport=139 protocol=tcp new
enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Session-In)" profile=public dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Session-In)" profile=private dir=in localport=139 protocol=tcp
new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Session-In)" profile=public,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
```

```
Session-In)" profile=private,domain dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Session-In)" profile=private,public dir=in localport=139
protocol=tcp new enable=no
netsh advfirewall firewall set rule name="파일 및 프린터 공유(NB-
Session-In)" profile=any dir=in localport=139 protocol=tcp new
enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=public dir=in localport=445 protocol=tcp new
enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=private dir=in localport=445 protocol=tcp new
enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=public,domain dir=in localport=445 protocol=tcp
new enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=private,domain dir=in localport=445 protocol=tcp
new enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=private,public dir=in localport=445 protocol=tcp
new enable=no
```

```
netsh advfirewall firewall set rule name="파일 및 프린터 공유(SMB-
In)" profile=any dir=in localport=445 protocol=tcp new
enable=no
```

```
}
'en-US'
```

```
{
Write 'OS Version'
```

```
[Environment]::OSVersion
```

```
Write-Verbose -Message "Vulnerability Port Removal UDP 137,
UDP 138, TCP 139, TCP 445" -Verbose
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=public dir=in localport=137 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private,domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=private,public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Name-In)" profile=any dir=in localport=137 protocol=udp
new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=public,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private,domain dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=private,public dir=in
localport=137 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Name-In)" profile=any dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public,domain dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, domain dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, public dir=in localport=137
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=any dir=in localport=137
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=public, domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private, domain dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=private, public dir=in
localport=138 protocol=udp new enable=no
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Datagram-In)" profile=any dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=public, domain dir=in localport=138
protocol=udp new enable=no
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private, domain dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=private,public dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Network Discovery
(NB-Datagram-In)" profile=any dir=in localport=138
protocol=udp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=public dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=private dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=public,domain dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=private,domain dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=private,public dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="Virtual Machine
Monitoring (NB-Session-In)" profile=any dir=in localport=139
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=public dir=in localport=139
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=private dir=in localport=139
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=public,domain dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=private,domain dir=in
localport=139 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File and Printer
Sharing (NB-Session-In)" profile=private,public dir=in
localport=139 protocol=tcp new enable=no
```



```
netsh advfirewall firewall set rule name="File and Printer  
Sharing (NB-Session-In)" profile=any dir=in localport=139  
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=public dir=in localport=445  
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=private dir=in localport=445  
protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=public,domain dir=in  
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=private,domain dir=in  
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=private,public dir=in  
localport=445 protocol=tcp new enable=no
```

```
netsh advfirewall firewall set rule name="File Server Remote  
Management (SMB-In)" profile=any dir=in localport=445  
protocol=tcp new enable=no
```

```
}
```

```
}
```