# Privilege Escalation Vulnerability Windows Defender Task

# CVE-2015-0098

April 14, 2015

Classification:
Public

CVE-2015-0098

IOprotect GmbH
Huobstrasse 14
8808 Pfäffikon SZ
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

## Vulnerable Windows Defender Task

| | |
|---|---|
| Advisory publication: | April 14, 2015 |
| Vendor Notification: | November 12, 2014 |
| Vulnerability Class: | Local privilege escalation |
| Affected Platform: | Windows 7 for 32-bit Systems Service Pack 1<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 |

## Advisory Details:

IOprotect identified a privilege escalation vulnerability in the Windows Defender Task on some installations of Windows 7 and Windows Server 2008. The task runs under the context of SYSTEM and is trying to launch the following binary:

```
D:\Program Files\Windows Defender\MpCmdRun.exe
```

The path points to the D: drive, but that drive does not exist. IOprotect reported the finding to Microsoft in November 2014. After investigating the issue, Microsoft confirmed it as an exploitable vulnerability.

## Impact

If D:  points to the CD ROM drive, the attack is only possible with physical access to the system. In scenarios where the D: drive does not exist, any local user or malicious code can create a virtual D: drive and place a specially crafted binary at the location mentioned above. This is an easy exploitable privilege escalation path, as the Windows Defender Task runs under the context of SYSTEM.

## Recommendations

It is recommended to install the Patch available from Microsoft:
https://technet.microsoft.com/library/security/MS15-037