|  |
| --- |
| Consalud S.A |
| Reporte Vulnerabilidades |
| Correspondientes a boletines Microsoft |
|  |
| **Francisco Abarca** |
| **22/01/2019** |

|  |
| --- |
| En este reporte se encontrarán las métricas correspondientes al sondeo de parches de seguridad de ciertas vulnerabilidades, este reporte será útil para crear un plan de contingencia sobre actualizaciones de las máquinas y las brechas de seguridad nativas vigentes. |

Contenido

[MS17-010 2](#_Toc535915084)

# MS17-010

10/10/2017

**Descripción:** Esta actualización de seguridad resuelve vulnerabilidades, las cuales permiten la ejecución de código de manera remota si el atacante envía mensajes creados especialmente a un servidor SMBv1 (Server Message Block).

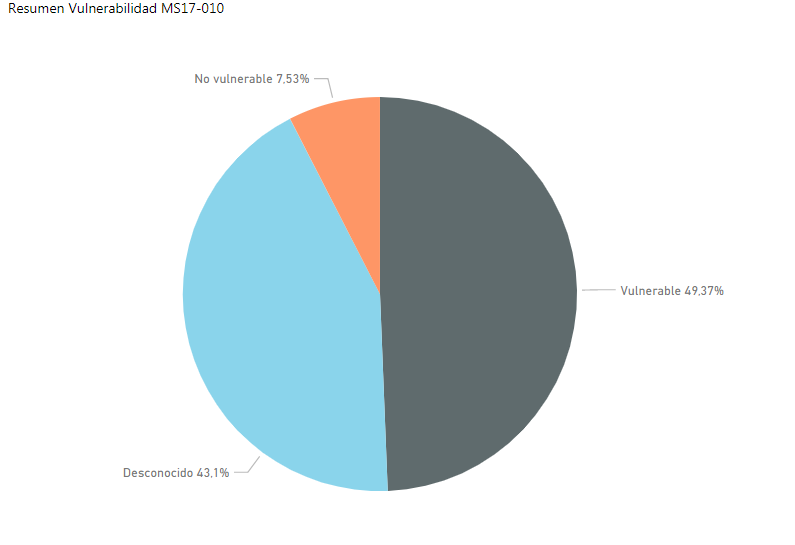
**Detalle Vulnerabilidades**

* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143
  + [**Crítica**] Ejecución de código de forma remota
* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144
  + [**Crítica**] Ejecución de código de forma remota
* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145
  + [**Crítica**] Ejecución de código de forma remota
* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146
  + [**Crítica**] Ejecución de código de forma remota
* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0147
  + [**Importante**] Revelación de información
* Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148
  + [**Crítica**] Ejecución de código de forma remota

**Afectados**

* Windows Vista
  + Vista SP 2 [KB4012598]
  + Vista x64 SP2 [KB4012598]
* Windows Server 2008
  + Server 2008 x86 SP2 [KB4012598]
  + Server 2008 x64 SP2 [KB4012598]
  + Server 2008 Itanium [KB4012598]
* Windows 7
  + 7 x86 SP1 [KB4012212] [Sólo Seguridad]
  + 7 x86 SP1 [KB4012215] [Mensual]
  + 7 x64 SP1 [KB4012212] [Sólo Seguridad]
  + 7 x64 SP1 [KB4012215] [Mensual]
* Windows Server 2008 R2
  + Server 2008 R2 x64 SP1 [KB4012212] [Sólo Seguridad]
  + Server 2008 R2 x64 SP1 [KB4012215] [Mensual]
  + Server 2008 R2 Itanium SP1 [KB4012212] [Sólo Seguridad]
  + Server 2008 R2 Itanium SP1 [KB4012215] [Mensual]
* Windows 8.1
  + 8.1 x86 [KB4012213] [Sólo Seguridad]
  + 8.1 x86 [KB4012216] [Mensual]
  + 8.1 x64 [KB4012213] [Sólo Seguridad]
  + 8.1 x64 [KB4012216] [Mensual]
* Windows Server 2012 y Windows Server 2012 R2
  + Server 2012 [KB4012214] [Sólo Seguridad]
  + Server 2012 [KB4012217] [Mensual]
  + Server 2012 R2 [KB4012213] [Sólo Seguridad]
  + Server 2012 R2 [KB4012216] [Mensual]
* Windows RT 8.1
  + RT 8.1 [KB4012216] [Mensual]
* Windows 10
  + 10 x86 [KB4012606]
  + 10 x64 [KB4012606]
  + 10 Version 1511 x86 [KB4013198]
  + 10 Version 1511 x64 [KB4013198]
  + 10 Version 1607 x86 [KB4013429]
  + 10 Version 1607 x64 [KB4013429]
* Windows Server 2016
  + Server 2016 x64 [KB4013429]
* Server Core Installation
  + Server 2008 x86 SP2 [KB4012598]
  + Server 2008 x64 SP2 [KB4012598]
  + Server 2008 R2 x64 SP1 [KB4012212] [Sólo Seguridad]
  + Server 2008 R2 x64 SP1 [KB4012215] [Mensual]
  + Server 2012 [KB4012214] [Sólo Seguridad]
  + Server 2012 [KB4012217] [Mensual]
  + Server 2012 R2 [KB4012213] [Sólo Seguridad]
  + Server 2012 R2 [KB4012216] [Mensual]
  + Server 2016 x64 [KB4013429]

**Estado[[1]](#footnote-1) [233 Servidores Analizados]**



1. Para un análisis más detallado revisar documento Excel adjunto en la hoja con nombre “MS17-010” [↑](#footnote-ref-1)