

Forum:[Hack Forums](#)

Thread: [Securing a Windows Environment Against Remote Attacks](#)

veiled - May 29, 2020, 12:32 pm

Disable RPC calls.

here are the core services that depend on rpc

Code Background Intelligent Transfer Service

COM+ Event System

Distributed Link Tracking Client

Distributed Transaction Coordinator

Fax Service

Indexing Service

IPSec Policy Agent

Messenger

Network Connections

Print Spooler

Protected Storage

Removable Storage

Routing Information Protocol (RIP) Listener

Routing and Remote Access

Task Scheduler

Telephony

Telnet

Windows Installer

Windows Management Instrumentation

In an Enterprise network, honestly, you wouldn't really need RPC calls for any business essential features.

13uNkNoWn - May 31, 2020, 12:27 pm

(May 29, 2020 12:32 PM)veiled Wrote: [\[CITE\]](#) Disable RPC calls.

In an Enterprise network, honestly, you wouldn't really need RPC calls for any business essential features.

lol.. you want to check your information, if you really believe this.

I would fire you on the spot if you were a sysadmin and said this to me.

Ampere - May 31, 2020, 12:59 pm

Pretty incorrect since the majority of SysAdmin tasks rely on some basic RPC functions such as Network Connections and WMIC for enterprise system management.

You're better off securing against untrusted RPC Calls then removing them entirely.

veiled - June 1, 2020, 10:13 am

Quote:lol.. you want to check your information, if you really believe this.

I would fire you on the spot if you were a sysadmin and said this to me.

Luckily I'm not a system administrator.