1.5.2 Ensure XD/NX support is enabled (Not Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

Rationale

Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Audit

Run the following command and verify your kernel has identified and activated NX/XD protection.

```
# dmesg | grep NX
NX (Execute Disable) protection: active
```

Remediation

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems.
If necessary configure your bootloader to load the new kernel and reboot the system.
You may need to enable NX or XD support in your bios.

Notes

Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.