National Cyber Security Centre

20 July 2012

NCSC Security Advisory – NCSC-ADV-201207-001

Product Support

The purpose of this advisory is to highlight the importance of using vendor-supported or community-supported products for ICT networks and systems.

In line with best practice, and in some instances policy, all hardware and software products should be patched with the latest bug fixes and security updates to address known vulnerabilities and provide protection against security exploits. Patches are regularly issued for supported products and these should be installed on a timely basis.

It is inevitable that all products will be superseded and eventually become obsolete. End-of-life (EOL) is the term typically used when a product is considered to be at the end of its useful lifetime and will no longer be manufactured or marketed. In some cases EOL also means a reduction in the level of support for a product.

End-of-support (EOS) refers to the date after which support for a product will no longer be available. Unless specific arrangements are in place, EOS means the cessation of technical assistance, bug fixes and security updates.

EOL and EOS are usually announced well in advance and support for a product can continue for some months (even years) after the EOL date.

Use of obsolete, unsupported products increases security risks and may introduce other risks.

The cost of replacing unsupported products may prove to be quite significant. However, the damage to a commercial or government organisation resulting from a successful cyber-attack can potentially cost a great deal more.

It is strongly advised that organisations only use supported products.

Where circumstances preclude using vendor-supported or community-supported products then compensatory controls should be considered.

PO Box 12-209, Wellington, New Zealand | info@ncsc.govt.nz | Phone: +64 4 4987654 | Fax: +64 4 4987655