Written by Marco Attard
31 January 2013

Following a whitepaper from security specialists Rapid 7 the US Department of Homeland Security issues a networking security warning-- hackers might exploit flaws in the Universal Plug and Play (UPnp) protocol.

According to Rapid7 common UPnP discovery protocol (SSDP) implementations, such as the UPnP control interface (SOAP) and the libupnp open source portable UPnP device SDK, have a number of bugs allowing the ill-intentioned to crash services and execute arbitrary code.

In other words, wannabe hackers might be able to steal sensitive data, run DDOS attacks or take full control over PCs and connected devices.

The US Computer Emergency Readiness Team (US-CERT) suggests users should "disable UPnP (if possible)" while vendors obtain and implement libupnp version 1.6.18, which addresses the vulnerabilities.

Rapid7 warns up to 50 million devices are vulnerable to the flaws (or 6900 products from 1500 vendors), including Windows, Apple and Linux PCs and mobile devices connecting to wireless or networked printers.

Go Security Flaws in UPnP: Unplog, Don't Play (Rapid7)

Go [US Government Warns of Hack Threat to Network Gear (Reuters)]