NEWS RELEASE

UPnP Forum Responds to Recently Identified LibUPnP/MiniUPnP Security Flaw

Beaverton, Ore., USA – 8 February 2013: UPnP Forum – the global standards body that has paved the way for seamless connectivity between more than a billion devices – today responds to concerns over a security flaw identified by Rapid7 in the open source, third party libraries ‘libupnp’ hosted at SourceForge and MiniUPnP hosted at miniupnp.free.fr.

On January 29th, UPnP Forum members received the public news that Rapid7 has identified a security flaw in the open source, 3rd party stacks libupnp and MiniUPnP. Based on Rapid7’s white paper, the flaw is only in the implementation of old versions of libupnp (older than 1.6.18) and MiniUPNP (older than 1.4). The flaws are NOT associated with the UPnP specifications themselves or UPnP Forum’s certification process for UPnP stacks. In addition, the flaws outlined by Rapid 7 show an implementation responding to UPnP protocols on the WAN ports of routers that existing UPnP standards are not designed for. Existing UPnP protocols are only intended for LAN usage that is not forwarded on to the internet.

The UPnP Forum is encouraging all vendors using open source implementations of protocol stacks to ensure they are using the latest releases and are active in ensuring that the security of those stacks is maintained. In the case of the libupnp and MiniUPnP, the UPnP Forum has posted a message to its website to help consumers and vendors identify the problem in this third party software. Please note that other issues have been identified in the latest version of MiniUPnP, 1.4, but they won't be publicly disclosed until the library's developer releases a patch to address them, so we advise caution on any further usage of this stack until such time. We are also looking into test tool enhancements that can identify implementations coming for certification that continue to use this flawed older versions of UPnP stacks. Numerous other closed and open source stacks exist in the UPnP ecosystem to use as alternatives if you have remaining concerns over libupnp or MiniUPNP.

For gateway vendors both affected and unaffected by this identified flaw, the UPnP Forum continues to advise that vendors implement the latest version of the Internet Gateway Device (v2) rather than the V1 that is deployed today. Along with our Device Protection standard, this specification provides numerous enhancements for security as well as necessary enhancements like the growing deployment of IPv6.

For further information about UPnP Forum please go to www.upnp.org. For general questions, please e-mail upnpfeedback@forum.upnp.org.

###

About UPnP Forum
UPnP Forum, established in 1999, is a global alliance of more than 950 industry-leading organizations working to enable device-to-device interoperability and facilitate easier and better home networking. The Forum promotes the adoption of uniform technical device interconnectivity standards and certifies devices conforming to these standards. UPnP Forum is an impartial group enabling member companies to participate and develop extensions to the UPnP Device Architecture, which defines how to use the Internet Protocol (IP) to communicate between devices, and Device Control Protocols (DCPs), which are services between devices. Members of UPnP Forum include market leaders in computing, printing and networking, consumer electronics, home appliances, automation, control and security, and mobile products.

For media enquiries please contact:
Dana Corson
Proactive PR
dana.corson@proactivepr.com
Tel: +44 1636812152
Mobile: +44 7795 615466