LIONIC®
Security Chip Provider

04/02/2013
Doc No: SN-2013-06003

Security News

2013-06003 Portable SDK for UPnP Devices (libupnp) Contains Multiple Buffer Overflow Vulnerabilities in SSDP

1. Affected Version

Portable SDK 1.2.1a ~ 1.8.0
Intel SDK 1.2

2. Description

Universal Plug and Play (UPnP) is a set of network protocols designed to support automatic discovery and service configuration. The Portable SDK for UPnP Devices (libupnp) is an open source project that has its roots in the Linux SDK for UPnP Devices and software from Intel (Intel Tools for UPnP Technologies and later Developer Tools for UPnP Technologies). Intel no longer maintains or supports these tools. Many different vendors produce UPnP-enabled devices that use libupnp.

Multiple buffer overflow vulnerabilities have been identified in Portable SDK for UPnP Devices libupnp library.

3. Vulnerability Analysis

The libupnp library is vulnerable to multiple stack-based buffer overflows when handling malicious SSDP requests. The vulnerable **unique_service_name** function in ssdp/ssdp_server.c in the SSDP parser in the portable SDK for UPnP Devices allows remote attackers to execute arbitrary code or cause a denial of service via **a long DeviceType**(aka urn), **a long UDN** (aka device) or **a long ServiceType**(aka urn service) field in a **UDP packet**.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 04/02/2013.
2. Apply an Update:

   libupnp 1.6.18 has been released to address these vulnerabilities.
3. Restrict Access

Deploy firewall rules to block untrusted hosts from being able to access **port 1900/udp**.

4. Disable UPnP:

   Consider disabling UPnP on the device if it is not absolutely necessary.

5. Reference

1. http://www.kb.cert.org/vuls/id/922681
2. CVE-2012-5958, CVE-2012-5961, CVE-2012-5962, CVE-2012-5964, CVE-2012-5965
3. Rapid7 advisory.