SOC Threat Advisory Threat Level – Significant
Network Time Protocol Daemon (ntpd)

This is to reference the Network Time Protocol Daemon (ntpd)
07/06/16

Synopsis
The Network Time Protocol Daemon (ntpd) is an operating system program that maintains the system time in synchronization with time servers using the Network Time Protocol (NTP).

NTP.org's reference implementation of NTP server, NTPD, contains multiple vulnerabilities. The vulnerabilities include 1 high severity and 4 low severity vulnerabilities.

Technical Threat

The new vulnerabilities that have been released are as follows:

- Network Time Protocol CRYPTO-NAK denial of service (CVE-2016-4957) (Sec 3046)
  The security hole was introduced by the fix for CVE-2016-1547, an issue patched in April.
- This vulnerability is related to the processing of crypto NAK packets and it can be exploited by an off-path attacker to cause a pre-emptible client association to be demobilized.
- Bad authentication demobilizes ephemeral associations (CVE-2016-4953) (Sec 3045)
- Processing of spoofed server packets affects variables (CVE-2016-4954) (Sec 3044)
- Autokey associations may be reset when repeatedly receiving spoofed packets. (CVE-2016-4955) (Sec 3043)
- Broadcast associations are not covered in Sec 2978 patch, which may be leveraged to flip broadcast clients into interleave mode. (CVE-2016-4956) (Sec 3042)

Impact

The impact of any of these 5 vulnerabilities being exploited would be that remote attackers may be able to spoof or send specially crafted packets to create denial of service like conditions.

The following Vendors have been notified of the vulnerabilities.

Remediation & Mitigation

Version 4.2.8p8 has been released to address these issues. Users are encouraged to update to the latest version. Those unable to update should consider mitigations listed in NTP's security Advisory listing.

Further Reading:

http://support.ntp.org/bin/view/Main/SecurityNotice#June_2016_ntp_4_2_8p8_NTP_Securi

http://www.kb.cert.org/vuls/id/321640

For more information, please contact:

Fujitsu Managed Security Services

fapl.askMSS@sg.fujitsu.com