March 10, 2014

To: CIOs
(A TECH version of this Alert is available [6])

REN-ISAC ALERT:
NTP-Based Distributed Denial of Service Attacks – Prevent your institution from being an unwitting partner in these attacks

The REN-ISAC [1] wants to raise awareness and drive change concerning common network time protocol (NTP) and network configurations that fall short of best practices and which, if left uncorrected, open the door for your institution to be exploited as an unwitting partner in delivering crippling distributed denial of service (DDoS) attacks against third parties.

The higher education and research community needs to do its part to ensure that we are not helping to facilitate these attacks. The REN-ISAC recommends the following:

=== **ACTIONS** ===

1. Distribute a copy of the TECH version [6] of this message to your network administrators, information security staff, system administrators, and other relevant personnel.

2. Identify hosts on your network with ntpd installed and running. Disable "monlist" capabilities on those NTP servers. Or, for systems which cannot be updated or configured to eliminate the monlist risk, apply network filters to prevent external requests to these insecure systems.

3. Ensure your institutional networks are unable to originate Internet traffic with spoofed source addresses.

==========

Although DDoS attacks exploiting the NTP and network configuration weaknesses have been around for a long time, the frequency and impact of these attacks have grown over the past year. The traffic sourced by any single system may be small enough to go unnoticed at an institution, however, the aggregate traffic from many sources, as experienced at the target, can be crippling. Recent attacks [2,3,4] average around 7.3 gigabits per second of traffic aimed at the victim organization – more than the full Internet bandwidth of most small and medium-sized colleges and universities.

Given the history and success of recent attacks, we expect these attacks will rise in frequency and magnitude in the months ahead.

There are two issues:

1. NTP is a protocol used to synchronize the clocks of networked devices. A deprecated command, "monlist", permits a requesting computer to receive information regarding the last 600 connections made to the NTP server. A small input request can generate a large response.

   When a malicious actor spoofs the source IP address of a victim targeted for attack, and repeatedly sends monlist requests to thousands of insecure NTP servers located all over the Internet, an avalanche of traffic is directed at the victim, overwhelming the victim's network capacity.

   Monlist has been removed from newer versions of NTP and monlist can (and should) be disabled in older versions.

   The NTP issue is complicated by the fact that not only is NTP running on upgradeable enterprise servers, NTP is also employed on infrastructure devices and embedded systems in your enterprise, some of which can be updated only with great difficulty and expense. Concerning these "difficult" systems, network firewalls may be one approach that can be used to mitigate the problem of these vulnerable-but-uncorrectable devices.

2. The second issue, the network configuration issue, involves the problem of traffic with forged apparent source addresses. Systems on your network should not be able to transmit packets that appear to be from a source IP address that doesn't belong to you -- your systems should only originate traffic with accurate source IP information.

In addition to the problem of educational institutions being leveraged as the sources of attacks against third parties, there have been incidents of institutions being targeted as the victim of DDoS attacks. Best practices for mitigating DDoS attacks against your institution apply: know in advance how to partner with your ISP to mitigate the effects of an attack; concerning Internet2, refer to the "DDoS Attacks Policy" [5]. DDoS mitigation services are also available from commercial organizations.

A TECH version of this Alert with technical depth has been shared to campus IT security officers, and network and system administrators. Print-friendly copies of this Alert and the companion TECH version (with clobber-free long URLs) are available at the REN-ISAC web site:
http://www.ren-isac.net/alerts.html.

We'd appreciate your input on additional means to protect from this threat, and general feedback concerning this Alert. If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Special thanks go to the members of the REN-ISAC Technical Advisory Group (TAG) [7].

On behalf of the REN-ISAC team,

Doug Pearson
dodpears@ren-isac.net
Technical Director, REN-ISAC
http://www.ren-isac.net
24x7 Watch Desk +1(317)278-6630

==========
References
==========

[1] REN-ISAC
http://www.ren-isac.net

[2] Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks
http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

[3] DoS attacks that took down big game sites abused Web's time-sync protocol
http://arstechnica.com/security/2014/01/dos-attacks-that-took-down-big-game-sites-abused-webs-time-synch-protocol/

[4] NTP reflection attack
https://isc.sans.edu/diary/NTP+reflection+attack/17300

[5] Internet2 DDoS Attacks Policy
https://wiki.internet2.edu/confluence/display/network/Forms%2C+Maps%2C+Policies%2C+and+Procedures

[6] TECH version of this alert
http://www.ren-isac.net/alerts/REN-ISAC_Alert_NTP_Amp_DDoS_TECH_201403.html

[7] REN-ISAC Technical Advisory Group
http://www.ren-isac.net/about/advisory.html#technical

-o0o-