



State of Alaska State Security Office

State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

December 19, 2014

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2014-091

DATE(S) ISSUED:

12/19/2014

SUBJECT:

Multiple Vulnerabilities in Network Time Protocol daemon Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in the Network Time Protocol daemon (ntpd). The Network Time Protocol daemon is a time synchronization service commonly implemented in Linux based operating systems.

Successful exploitation could result in an attacker gaining the same privileges as the ntpd process. Depending on the privileges associated with the process, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

THREAT INTELLIGENCE:

At this time, these vulnerabilities have been publicly disclosed.

SYSTEMS AFFECTED:

- ntpd versions 4.2.7 and prior

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **N/A**

TECHNICAL SUMMARY:

Three buffer overflow vulnerabilities, one insufficient entropy security weakness, one predictable random number generator weakness and one missing return on error issue have been identified in Network Time Protocol daemon (ntpd). The three buffer overflow vulnerabilities could allow remote code execution.

- One buffer overflow vulnerability exists in the `crypto_rcv()` function that may be exploited via a specially crafted packet when the `ntp.conf` file contains a "crypto pw" directive. This vulnerability can be taken advantage by a remote unauthenticated attacker. (CVE-2014-9295)
- Two buffer overflow vulnerabilities exist, one in the `ctl_pdu_data()` function and one in the `configure()` function, that may be exploited via a specially crafted packet. These vulnerabilities can be taken advantage by a remote unauthenticated attacker. (CVE-2014-9295)
- One weak default key vulnerability exists in the `config_auth()` function when the "auth" key is set in the configuration file that causes the generation of default keys with low entropy. This issue may be used by an attacker to guess the generated key, and possibly use it to send ntpdc query or configuration requests. (CVE-2014-9294)
- One predictable random number generator weakness exists that causes the generation of a weak seed which is used in generating MD5 keys. This issue is located in `util/ntp-keygen.c` and may be used by an attacker to guess MD5 keys that could be used to spoof a NTP client or server (CVE-2014-9293)

- One missing return on error issue exists in ntp_proto.c that allows for processing to continue when a specific rare error occurs. Little is known about this issue or its effects at this time. (CVE-2014-9296)

Successful exploitation of the buffer overflow vulnerabilities could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Update vulnerable products immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack

REFERENCES:

ntp.org:

<http://support.ntp.org/bin/view/Main/SecurityNotice>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9293>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9294>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9295>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9296>

CERT:

<http://www.kb.cert.org/vuls/id/852879>

Security Focus:

<http://www.securityfocus.com/bid/71757>

<http://www.securityfocus.com/bid/71758>

<http://www.securityfocus.com/bid/71761>

<http://www.securityfocus.com/bid/71762>