*** 北米連携センター情報***

2014 年 12 月 22 日

●NTP にコードの遠隔的実行可能にする脆弱性

【ArsTechnica, 2014/12/19】
　インターネット経由の時刻同期に使われる「Network Time Protocol (NTP) に遠隔的なコード実行に使われる危険がある深刻な脆弱性が複数発見された。
　国土安全保障省（DHS）が運営する産業制御システム・サイバー緊急事態対応チーム（ICS-CERT）によると、この脆弱性は NTP 4.2.7 までのバージョンに含まれており、技術力が高くないハッカーでも NTP daemon (NTPD) プロセスの権限で悪意のあるコードを実行することが可能になるという。
　1 月にゲーム・サイトをターゲットに発生した DoS 攻撃では、この脆弱性を使った形跡が確認されている。
　脆弱性は、更新された NTP 4.2.8 では修正された。

記事入手元：
http://arstechnica.com/security/2014/12/attack-code-exploiting-critical-bugs-in-net-time-sync-puts-servers-at-risk/

（参考）本件報道記事
Attack code exploiting critical bugs in net time sync puts servers at risk

Updates available for remote code-execution vulnerabilities. Patch now!
by Dan Goodin - Dec 19 2014, 8:06pm -0500

Several critical vulnerabilities in the protocol implementation used to synchronize clock settings over the Internet are putting countless servers at risk of remote hijacks until they install a security patch, an advisory issued by the federal government warned.

The remote-code execution bugs reside in versions of the network time protocol prior to 4.2.8, according to an advisory issued Friday by the Industrial Control Systems Cyber Emergency Response Team. In many cases, the vulnerabilities

can be exploited remotely by hackers with only a low level of skill.

"Exploitation of these vulnerabilities could allow an attacker to execute arbitrary code with the privileges of the [network time protocol daemon] process," the advisory warned. Exploit code that targets the vulnerabilities is publicly available. It's not clear exactly what privileges NTP processes get on the typical server, but a handful of knowledgeable people said they believed it usually involved unfettered root access. Even if the rights are limited, it's not uncommon for hackers to combine exploits with privilege elevation attacks, which increase the system resources a targeted app has the ability to control.

Never-before-seen technique abused the Network Time Protocol to worsen effects.
In January, researchers uncovered evidence NTP was being exploited to wage crippling denial-of-service attacks on gaming sites. Attackers were using the widely used service to amplify the amount of bandwidth available to them, a technique that saturated targets with as much as 100 gigabits of data per second.

The bugs were discovered by Google Security Team researchers Neel Mehta and Stephen Roettger, who reported them privately. The vulnerabilities have been fixed in version 4.2.8. Maintainers of the open-source NTP code have bare-bones details on the bugs here. Additional details, including about separate information disclosure vulnerabilities caused by a weak default key and non-cryptographic random number generator in NTP, are here.

Post updated to add "implementation" to the first sentence.

以　上