AMIDST ALL OF the confusion and concern over an encryption algorithm that may contain an NSA backdoor, RSA Security released an advisory to developer customers today noting that the algorithm is the default in one of its toolkits and strongly advising them to stop using the algorithm.

The advisory provides developers with information about how to change the default to one of a number of other random number generator algorithms RSA supports and notes that RSA has also changed the default on its end in BSafe and in an RSA key management system.

The company is the first to go public with such an announcement in the wake of revelations by the New York Times that the NSA may have inserted an intentional weakness in the algorithm — known as Dual Elliptic Curve Deterministic Random Bit Generation (or Dual EC DRBG) — and then used its influence to get the algorithm added to a national standard issued by the National Institute of Standards and Technology.

http://www.wired.com/2013/09/rsa-advisory-nsa-algorithm/
In its advisory, RSA said that all versions of RSA BSAFE Toolkits, including all versions of Crypto-C ME, Micro Edition Suite, Crypto-J, Cert-J, SSL-J, Crypto-C, Cert-C, SSL-C were affected.

In addition, all versions of RSA Data Protection Manager (DPM) server and clients were affected as well.

The company said that to “ensure a high level of assurance in their application, RSA strongly recommends that customers discontinue use of Dual EC DRBG and move to a different PRNG.”

RSA is currently doing an internal review of all of its products to see where the algorithm gets invoked and to change those. A company spokesman said the review is expected to be completed next week.

“Every product that we as RSA make, if it has a crypto function, we may or may not ourselves have decided to use this algorithm,” said Sam Curry, chief technical officer for RSA Security. “So we’re also going to go through and make sure that we ourselves follow our own advice and aren’t using this algorithm.”

One product that is not affected by the algorithm is RSA’s SecurID system, which provides two-factor authentication for logging into networks. It requires users to enter a secret code number displayed on a key fob, or in software, in addition to their password when they log into their networks. The number is cryptographically generated and changes every 30 seconds. But a source close to RSA tells WIRED that neither the SecurID hardware tokens or software use this algorithm. Instead they use a different FIPS-certified random-number generator.

Curry told WIRED that the company added the Dual EC DRBG algorithm to its libraries in 2004 and 2005 at a time when elliptic curve algorithms were becoming the rage and were considered to have advantages over other algorithms. The algorithm was approved by NIST in 2006 for a standard governing random number generators.

http://www.wired.com/2013/09/rsa-advisory-nsa-algorithm/
BSafe has six random number generators in it, some are hash-based and several that are elliptic-curve based, like the algorithm in question. Curry says they chose Dual EC DRBG as the default “on the basis of providing the best security for our customers.”

The algorithm he said had features that gave it advantages over the others.

“The ability to do continuous testing of output, for instance, or the ability to do general sort of prediction resistance and to be able to do re-seeding,” he said. “Those are really attractive features.”

**Update 9.20.13:** To add information about RSA’s SecurID.

The advisory to RSA developers reads as follows:

Due to the debate around the Dual EC DRBG standard highlighted recently by the National Institute of Standards and Technology (NIST), NIST re-opened for public comment its SP 800-90 standard which covers Pseudo-random Number Generators (PRNG).

For more information about the announcement see:

http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-90-A%20Rev%201%20B%20and%20C

The ITL Security Bulletin mentioned in this announcement includes the following:

“Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: NIST strongly recommends that, pending the resolution of the security concerns and the re-issuance of SP 800-90A, the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used.”

The currently released and supported versions of the BSAFE libraries (including Crypto-J 6.1.x and Crypto-C ME 4.0.x) and of the RSA DPM clients and servers use Dual EC DRBG as the default PRNG, but most libraries do support other PRNGs
that customers can use. We are providing guidance to our customers on how to change the PRNG from the default in their existing implementation.

In the current product documentation, RSA has provided technical guidance for RSA BSAFE Toolkits and RSA DPM customers to change the PRNG in their implementation.

RSA will change the default RNG in RSA BSAFE Toolkits and RSA DPM as appropriate and may update the algorithm library as needed.

Republished for educational purposes only.

http://www.wired.com/2013/09/rsa-advisory-nsa-algorithm/