

[Products](#)[Services](#)[Publications](#)[Resources](#)[What's new](#)

[Follow @Openwall on Twitter for new release announcements and other news](#)

[\[<prev\]](#) [\[next>\]](#) [\[thread-next>\]](#) [\[day\]](#) [\[month\]](#) [\[year\]](#) [\[list\]](#)

Message-Id: <20150520182939.388A76C0029@smtpvmsrv1.mitre.org>
Date: Wed, 20 May 2015 14:29:39 -0400 (EDT)
From: cve-assign@...re.org
To: oss-security@...ts.openwall.com
Cc: cve-assign@...re.org
Subject: CVE-2015-4000 - TLS does not properly convey server's ciphersuite choice

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

CVE-2015-4000 has been assigned to this vulnerability in the TLS protocol that was disclosed in section 3.2 of the <https://weakdh.org/imperfect-forward-secrecy.pdf> paper:

"a flaw in the way TLS composes DHE and DHE_EXPORT. When a server selects DHE_EXPORT for a handshake, it proceeds by issuing a signed ServerKeyExchange message containing a 512-bit p512, but the structure of this message is identical to the message sent during standard DHE ciphersuites. Critically, the signed portion of the server's message fails to include any indication of the specific ciphersuite that the server has chosen."

(This is the TLS protocol problem associated with the Logjam attack.)

There are some other vulnerabilities mentioned on the weakdh.org web site that can have individual CVE IDs for each affected codebase, if any researcher (or a vendor) identifies a specific available codebase (i.e., not one organization's in-house code). Also, there are security issues mentioned on the weakdh.org web site that can have individual CVE IDs for each affected codebase, if the author of the code requires a CVE ID for announcing the issue to customers. Finally, there are other issues mentioned on the weakdh.org web site that should not have CVE IDs, but for which it is possible that someone is considering using CVE IDs. Here are some examples of this distinction.

section 3.5 - "some servers in our scans used Java's DSA primes as p, but mistakenly used the DSA group order q in the place of the generator g ... This substitution of q for g is likely due to a usability problem: the canonical ASN.1 representation of Diffie-Hellman key exchange parameters (coming from PKCS#3) is a sequence (p, g), while that of DSA parameters (coming from PKIX) is (p, q, g); we conjecture that the confusion between these formats led to a simple programming error."

[So, for example, if someone identifies a specific open-source product that has this programming error, a CVE ID can be assigned, even if the vendor's perspective is unknown.]

section 3.2 footnote - "Safari allowed groups as small as 16 bits"

[It seems that there's a high probability that this was unintentional behavior, and thus a CVE ID from Apple may be forthcoming.]

section 3 - "for both normal and export-grade Diffie-Hellman, the vast majority of servers use a handful of common groups"

[This is a type of issue that typically does not have a CVE ID because it is associated with the concept of third-party configuration data. Although we don't currently have complete documentation on what "third-party configuration data" means within CVE, the important points in this situation are:

1. Use of a common group obtained from a third party was not a choice that would have been anticipated to be unreasonable.
2. Avoiding use of a common group is not really equivalent to correcting a software mistake; it could typically involve improving a software product by adding new functionality or documentation, such as adding a call to "openssl dhparam" at installation time.
3. Existence of a common group across different customers' deployments of a product is not independently exploitable; there is no attack that depends exclusively on knowing the group used by a victim.

For example, it seems likely and appropriate that multiple vendors from the <https://weakdh.org/sysadmin.html> Common Server Products list, and a large number of other vendors, will adjust their own documentation (or installation process) to incorporate the general concept of "generate a new, unique Diffie-Hellman group." However, we don't feel that there should be CVE IDs to, in effect, track each vendor's progress toward this, or to criticize a vendor's choices (e.g., putting it only in documentation, with no new installation functionality). Instead, it can probably be treated as another important security improvement that becomes available to persons who pick up newer versions.]

- - -
CVE assignment team, MITRE CVE Numbering Authority
M/S M300
202 Burlington Road, Bedford, MA 01730 USA
[PGP key available through http://cve.mitre.org/cve/request_id.html]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.14 (SunOS)

```
iQEcBAEBAGAGBQJVXNGiAAoJEKllVAevmvsDlMH/3UC62Gsmk09BL7neAr9AKbX
sh/MtvC99+H0dIdiMKPACQiojR4MazFCaQNr6qQ+UCV7lXfaliHeJ4xi95U1Gdf3
EC5SQfwKSfbvIv7dR0HIa43MaS6MSSvshLcRfivpbyeYHfAU7Kj3AptIZ2LGsPTW
YMeZX0aEduNTE4QQJfk0xXsS5gW6mPNaqQm4MSggbzejR1B/wdcALjT2x0hhAxwQ
rjsx/xoMz6SWHx+J6gyOSIsTQ4B1ZwFszC22/3iXABJ/ZkYSuV/hQTa4AGXE/oKL
Qa11zenkraRvYmMLVynZWQkXsPrWUQ9A1gCjEllu0yDuNUbh2Y8+q3WA9oshhMM=
=2qz6
-----END PGP SIGNATURE-----
```

[Powered by blists - more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).