Message-ID: <CAA7hUgH2dCyNr0m_HmhLuVXO+ZD_TVOWdfrB-jzrLPnz7de4Dw@mail.gmail.com>
Date: Sat, 15 Jun 2019 17:09:53 +0200
From: Raphael Geissert <geissert@...ian.org>
To: Open Source Security <oss-security@...ts.openwall.com>
Cc: security@...tpractical.com
Subject: Apache::Session's use of md5 and more

Hi,

I just stumbled upon Apache::Session's Generate::MD5 module, which
appears to be used to generate the session ids for cookies and the
like.

Not only does it use MD5, but its source of entropy is weak and does
two rounds of hashing. From the source code[1]:

```
    $session->{data}->{_session_id} =
        substr(Digest::MD5::md5_hex(Digest::MD5::md5_hex(time(). {}.
rand(). $$)), 0, $length);
```

(where $length is 32 by default)

Am I missing something, or has this code actually been in use for ages
and gone unnoticed ? I couldn't find any CVE for this.

So far I found this reference, but only mentions the use of MD5 as a weakness:
https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/issues/695

>From a quick look at the reverse dependencies of the Debian package,
there are some users of Apache::Session:
* RequestTracker (RT) : from a quick look at the session id in the
cookie set by rt.cpan.org I'd say it does use Generate::MD5
* Torrus: no idea if the Generate::MD5 module is used
* LemonLdap::NG : they replaced Generate::MD5 by a similar code using
SHA256, but still using two rounds of hashing

CC'ing BestPractical. Will open an issue on LemonLdap::NG's gitlab.

[1]https://metacpan.org/source/CHORNY/Apache-Session-1.93/lib/Apache/Session/Generate/MD5.pm

Cheers,
--
Raphael Geissert - Debian Developer
www.debian.org