DuckCorp Infrastructure - Bug #513

Mailman: DMARC checks are enabled and could fail

2017-02-28 14:08 - Pierre-Louis Bonicoli

Status:	Resolved	**Start date:**	2017-02-28
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Service :: Mail	**Estimated time:**	0:00 hour
Target version:			
Patch Available:		**Entity:**	DuckCorp
Confirmed:	Yes	**Security:**	No
Branch:		**Help Needed:**	Yes

Description

DMARC checks are enabled by Mailman.

When a DMARC policy is defined in the sender domain, mails can be rejected:

/var/log/mailman/vette

```
Feb 28 10:36:38 2017 (7194) DMARC lookup for no-reply@microsoft.com (_dmarc.microsoft.com) found p
=reject in _dmarc.microsoft.com. = v=DMARC1; p=reject; pct=100; rua=mailto:d@rua.agari.com; ruf=ma
ilto:d@ruf.agari.com; fo=1
Feb 28 10:36:38 2017 (7194) Message discarded, msgid: <40d1e0c8-6fe4-4fd6-acfc-5e359d1960b2@BN1AFF
O11OLC003.protection.gbl>
```

```
Received-SPF: None (protection.outlook.com: microsoft.com does not designate
 permitted sender hosts)
Authentication-Results: spf=none (sender IP is )
 smtp.mailfrom=no-reply@microsoft.com;
```

What puzzles me is what/who added the Received-SPF header in the rejected mail ?

References:

- https://tools.ietf.org/html/rfc7208#section-9

```
   The Received-SPF header field is a trace field (see [RFC5322],
      Section 3.6.7) and SHOULD be prepended to the existing header, above
      the Received: field that is generated by the SMTP receiver.
```

History

#1 - 2017-02-28 14:36 - Pierre-Louis Bonicoli

- Status changed from Rejected to In Progress

Because Authentication-Results header if above the Received header of BN1AFFO11HUB037.protection.gbl, the Authentication-Results header must have been added by BN1AFFO11HUB037.protection.gbl:

```
Received: from NAM01-BY2-obe.outbound.protection.outlook.com (mail-by2nam01on0065.outbound.protection.outlook.
com [104.47.34.65])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-SHA384 (256/256 bits))
    (No client certificate requested)
    by mx1.duckcorp.org (Postfix) with ESMTPS id 3vXZnh6mw4z2J7j
    for <duck@duckcorp.org>; Tue, 28 Feb 2017 11:39:19 +0100 (CET)
Authentication-Results: spf=none (sender IP is )
 smtp.mailfrom=no-reply@microsoft.com;
Received: from BN1AFFO11FD005.protection.gbl (10.58.52.55) by
 BN1AFFO11HUB037.protection.gbl (10.58.52.148) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.1.933.11; Tue, 28 Feb 2017 10:39:17 +0000
Received: from BL2FFO11WSS007 (207.46.163.209) by
 BN1AFFO11FD005.mail.protection.outlook.com (10.58.52.65) with Microsoft SMTP
 Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384) id
 15.1.933.11 via Frontend Transport; Tue, 28 Feb 2017 10:39:17 +0000
```

Because we don't do any SPF checks (I guess we should not trust SPF results of others), we should:

- either disable DMARC checks on Mailman
- or add SPF checks

I propose the former.

#2 - 2017-02-28 15:31 - Pierre-Louis Bonicoli

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

The configuration below had been added to /etc/mailman/mm_cfg.py:

```
# Remove 'domainkey-signature', 'dkim-signature', 'authentication-results'
# headers
REMOVE_DKIM_HEADERS = 2
# With newer version of Mailman, 3 will allow to rename headers.
# Rename 'domainkey-signature', 'dkim-signature', 'authentication-results'
# headers, using 'X-Mailman-Original-' prefix.
```

and applied using: systemctl restart mailman.service.