

XSS Vulnerability in Hastymail (ver. 2.1.1)

Title: XSS Vulnerability in Hastymail (ver. 2.1.1)
Release Date: 2011/11/22
Vulnerable Application: Hastymail (ver. 2.1.1)
Type: Cross Site Scripting
Level: High (Low/High/Critical)
CVSS: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

Dognædis Ref.: DGS-SEC-2
CVE Ref.: CVE-2011-4541
Other Ref.:
Discover Credits: CodeV - Code Analyzer
Bulletin Author(s): HTrovao
Contact: irt@dognædis.com

Nível de Acesso do Documento: Público

A informação expressa neste documento é propriedade da Dognædis. Pode ser, no entanto, lida, copiada, distribuída, impressa ou acedida por qualquer pessoa ou entidade, desde que os créditos da Dognædis sejam respeitados.

Document Access Level: Public

The information expressed in this document is property of Dognædis. Although can be disclosed, distributed, copied, read, used, printed or accessed by anyone, since all the Dognædis credits are respected.

Overview:

Hastymail2 is a full featured IMAP/SMTP client written in PHP. It's goal is to create a fast, secure, compliant web mail client that has great usability.

Scope:

File: /lib/ajax_functions.php

Vulnerable Argument(s): \$func_name (from \$_POST['rs'])

Code:

```
line 40: echo "--:$func_name not callable";
```

Proof(s) of Concept:

```
GET: http://<app_base>/index.php?page=mailbox&mailbox=Drafts  
POST: rs=<script>alert('xss')</script>
```

Description:

The referred vulnerability could be exploited through a XSS (Cross-Site-Scripting) attack.

Ultimately, the attacker could take complete control of the victims web-browser.

In a successful attack, the malicious script would be executed with the authenticated user permissions.

Impact:

Generally, by exploiting this kind of vulnerability, it might be possible to achieve possible attack vectors to various kinds of attacks such as:

- Session/Cookie theft
- Account Hijacking
- Identity theft
- Accessing confidential resources
- Accessing pay content
- Account Denial of service

Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the \$_POST['rs'] input argument should be properly sanitized for HTML and following ECMAS usage.

Official Solution:

Users are recommended to upgrade to the newer version (v2.1.1-RC2), which is available in the application website.

External References:

[http://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](http://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

[http://www.owasp.org/index.php/Cross-Site_Request_Forgery_\(CSRF\)](http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

http://en.wikipedia.org/wiki/Cross-site_scripting

http://en.wikipedia.org/wiki/Code_injection



DOGNÆDIS

TRUSTABLE SOLUTIONS