Title              SmarterMail - Stored XSS in emails
Release Date      6 March 2015
Reference          NCC00776
Discoverer         Soroush Dalili
Vendor             Smarter Tools
Systems Affected   v13.1.5451 and prior
CVE Reference      TBC
Risk               Medium
Status             Fixed

Resolution Timeline
Discovered         29 December 2014
Reported           9 February 2015
Released           30 December 2014
Fixed              26 February 2015
Published          6 March 2015

Vulnerability Description
The SmarterMail application was vulnerable to a stored cross-site scripting issue by bypassing the anti-XSS mechanisms. It was possible to run JavaScript code when a victim user opens or replies to the attacker's email, which contained a malicious payload. Therefore, users' passwords could be reset by using an XSS attack, as the password reset page did not need the current password.

Technical Details
The following payload could be used to run JavaScript code by opening an email:
<svg/onload=alert(1)></svg>

The following payload could be used to run JavaScript code by pressing the reply button:
<iframe src=javascript:alert(1)></iframe>

Fix Information
The issue was patched in Version 13.3.5535 (2015-02-26) which can be downloaded here: http://www.smartertools.com/smartermail/releasenotes/v13.aspx

Research          https://www.nccgroup.com/research
Twitter           https://www.twitter.com/NCCGroupInfoSec / @NCCGroupInfoSec
Open Source       https://github.com/nccgroup
SlideShare        http://www.slideshare.net/NCC_Group/