LIONIC®
Security Chip Provider

30/09/2011
Doc No: SN-2011-40017

Security News
2011-40017 Newgen Omnidocs Bypass Access Restriction Vulnerability

1. Affected Version

Newgen OmniDocs

2. Description

OmniDocs is an Enterprise Document Management (EDM) platform for creating, capturing, managing, delivering and archiving large volumes of documents and contents. It also integrates seamlessly with other enterprise applications.

Multiple bypass access restriction vulnerability has been reported in OmniDocs.

3. Vulnerability Analysis

The affected sample URL is listed as follows:

```
http://serverIP/omnidocs/doccab/doclist.jsp?DocListFolderId=927964&Folder-
Type=G&FolderRights=010000000&FolderName=1234&FolderOwner=test&FolderLocation=G
&FolderAccessType=I&ParentFolderIndex=100&FolderPathFlag=Y&Fetch=5&VolIndex=1&V
olIndex=1
```

Table 1: The affected sample URL

The vulnerability is caused due to OmniDocs Omnidocs application does't validate parameters. An attacker can modify 'FolderRights' parameter to '111111111' to get full access including rights to add documents, add folders, delete folders and place orders.

Also, OmniDocs allows remote attackers to bypass intended access restrictions via a modified 'UserIndex' parameter to doccab/userprofile/editprofile.jsp , which selects the settings page of an arbitrary user thereby gaining access to view or change other user's personal settings.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 29/09/2011.
2. Contact your vendor for an appropriate patch.

5. Reference

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3645