Sense of Security	Authorisation. Jason Edelstein
	Release date. 14 April 2015

Sense of Security – Security Advisory – SOS-15-003.

ClickSoftware ClickMobile Multiple Security Vulnerabilities

14 April 2015.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 14 April 2015

ClickSoftware ClickMobile - Security Advisory - SOS-15-003

Release Date.	14-Apr-2015
Last Update.	-
Vendor Notification Date.	24-Jun-2014
Product.	ClickSoftware ClickMobile Mobile Application
Platform.	iOS
Affected versions.	ClickMobile 8.1.9 (v17) and lower
Severity Rating.	High
Impact.	Privilege escalation Security bypass Manipulation of data
Attack Vector.	Remote with authentication
Solution Status.	Vendor patch
CVE reference.	-
SAP Security Notes	2111169

Details.

ClickSoftware ClickMobile is a mobile application which provides workforce management functionality to field engineers. The ClickMobile application has vertical and horizontal privilege escalation vulnerabilities which allow mobile users to impersonate other users by only knowing their username (without their password). The ClickMobile web service has no access control after the initial NTLM authentication exchange. Attackers can use this vulnerability to impersonate a privileged user to obtain unauthorised access to SAP resources or to manipulate SAP data which requires higher privileges.

ClickMobile also allows verifying the file extension, size, and amount being uploaded from the client side. Once this verification is performed on the client side and passed,

there is no ability to control the insertion of files into the MiddleTier DB. Whereby allowing the upload of insecure files.

Solution.

Install the 8.1.10 P2 Security Enhancement msi on the ClickMobile MiddleTier server.

Make the below configuration changes to fix the insecure file upload vulnerability:

1. On the MiddleTier IIS, open the Web.Config file.
2. Under the "appSettings" add the following 2 keys:

```
<add key="FileUploadPreprocessorDLLPath"
value="FileUploadCheck.dll"/>
```

(This is the DLL name which should be located under the bin folder of the ClickMobileWeb site)

```
<add key="FileUploadPreprocessorProgID"
value="FileUploadCheck.Preload"/>
```

(This is the <namespace>.<class name> of the code.)

3. Save the file.
4. Stop/Start the IIS process (W3WP).

Make the below configuration changes to fix privilege escalation and unauthorised access vulnerabilities:

1. On the MiddleTier IIS, open the Web.Config file.
2. Under "appSettings" add the following key:
   `<add key="ValidateUserInRequests" value="true"/>`
3. Save the file.
4. Stop/Start the IIS process (W3WP).

Discovered by.

Fatih Ozavci 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	Authorisation. Jason Edelstein
	Release date. 14 April 2015

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/consulting/SAP-security
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-15-003.pdf

Other Sense of Security advisories can be found at:

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