	Authorisation. Jason Edelstein
	Release date. 14 April 2015

Sense of Security – Security Advisory – SOS-15-004.

ClickSoftware ClickSchedule Multiple Security Vulnerabilities

14 April 2015.

ClickSoftware ClickSchedule - Security Advisory - SOS-15-004

Release Date.	14-Apr-2015
Last Update.	-
Vendor Notification Date.	24-Jun-2014
Product.	ClickSoftware ClickSchedule Web Application
Platform.	-
Affected versions.	-
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 ClickSchedule is a web application which provides workforce management and scheduling functionality to field engineers and managers. The ClickSchedule application and the backend web service have vertical and horizontal privilege escalation vulnerabilities which allow mobile users to impersonate other users by only knowing their username (without their password). The ClickSchedule web service which is connected with the web application itself has no access control after the initial NTLM authentication exchange. Also it uses the *CallerIdentity* and *ID* variables in requests as the user identity instead of the identity in the authenticated session data. This allows users to spoof their identities to manipulate the system logging or access control. Attackers can use these vulnerabilities to impersonate a privileged user to obtain unauthorised access to SAP resources or to manipulate SAP data which requires higher privileges.

Solution.

Install the 8.2 Patch002 Security Enhancement .msi and follow the vendor instructions contained in the security note.

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 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-15-004.pdf

Other Sense of Security advisories can be found at:

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