Sense of Security	Authorisation. Jason Edelstein
	Release date. 14 December 2014

Sense of Security – Security Advisory – SOS-14-005.

SAP NetWeaver Business Client for HTML Cross-site Scripting Vulnerabilities

14 December 2014.

SAP NetWeaver Business Client for HTML - Security Advisory - SOS-14-005

Release Date.	14-Dec-2014
Last Update.	-
Vendor Notification Date.	24-Jun-2014
Product.	SAP NetWeaver Business Client for HTML 3.0
Platform.	-
Affected versions.	SAP NetWeaver Business Client for HTML 3.0
Severity Rating.	Medium
Impact.	Manipulation of data
Attack Vector.	Remote without authentication
Solution Status.	Workaround
CVE reference.	-
SAP Security Notes	2051285

Details.

Multiple cross-site scripting vulnerabilities were detected in the SAP NetWeaver Business Client for HTML 3.0. The NetWeaver Business Client for HTML 3.0 can be abused by an attacker, allowing them to modify displayed application content without authorisation, and to potentially obtain authentication information from other legitimate users. SAP has released security notes and a workaround solution to mitigate the vulnerabilities.

Exploit.

https://customer.com/vendor/~testcanvas/?title=[Cross-site Scripting Data]&flags=&roundtrips=1+&sap-accessibility=&as_fid=nTEgMjp9nblZhLohXjDE

https://customer.com/vendor/~testcanvas/?title=&flags=&roundtrips=[Cross-site Scripting Data]

Solution.

NetWeaver Business Client for HTML 3.0 was never officially released for SAP_BASIS 720. Therefore it needs to be deactivated there.

Start the ABAP transaction SICF.

On the initial screen search for the service name "nwbc".

On the result page click on any of the listed NWBC nodes and deactivate them - via the context menu ("Disable Service") or via main menu (`Service/host --> Disable`).

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-14-005.pdf

Other Sense of Security advisories can be found at:

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