Sense of Security	Authorisation. Jason Edelstein
	Release date. 03 Apr 2013.

Sense of Security – Security Advisory – SOS-13-001.

Google Active Directory Sync Tool - Exposure of Sensitive Information Vulnerability.

03 Apr 2013.

Google Active Directory Sync Tool Vulnerability - Security Advisory - SOS-13-001

Release Date.	03-Apr-2013
Last Update.	-
Vendor Notification Date.	03-Sep-2012
Product.	Google Active Directory Sync (GADS) Tool
Platform.	Windows, Linux, Solaris
Affected versions.	All versions up to 3.1.3
Severity Rating.	High
Impact.	Exposure of sensitive information
Attack Vector.	From local without authentication
Solution Status.	Upgrade to version 3.1.6
CVE reference.	CVE - Not yet assigned

Details.

Due to a weakness in the way the Java encryption algorithm (PBEwithMD5andDES) has been implemented in the GADS tool all stored credentials can be decrypted into plain-text. This includes all of the encrypted passwords stored in any end-users saved XML configuration file, such as Active Directory accounts, SMTP, Proxy details, LDAP and OAuth tokens, etc.

Proof of Concept.

Using the following information from the XML and GADS tool to decrypt all encrypted passwords from any XML:

1. The hard coded salt:

```
SALT[] = { -87, -101, -56, 50, 86, 53, -29, 3 }
```

2. The hard coded DES interation count:

```
ITERATION_COUNT = 20
```

3. The Secret key derived from the uniqueID value in the XML:
   `6512630db9a74d90a5531f574b85f398`
4. The cipher-text from the XML:
   `<encryptedAdminPassword>1edOUtamjNA=</encryptedAdminPassword>`
5. The algorithm:
   `PBEwithMD5andDES`

The decrypted value is: winning!

Solution.

Install the latest version (3.1.6) of the Google Active Directory Sync tool.

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-13-001.pdf

Other Sense of Security advisories can be found at:

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