Sense of Security	Authorisation. Jason Edelstein
	Release date. 29 April 2013.

Sense of Security – Security Advisory – SOS-13-002.

Mi-Token Enterprise Edition & API Edition – Brute-Force Vulnerability

29 April 2013

Sense of Security	Authorisation. Jason Edelstein
	Release date. 29 April 2013.

Mi-Token Enterprise Edition & API Edition – Brute-force Vulnerability - Security Advisory - SOS-13-002

Release Date.	29-Apr-2013
Last Update.	-
Vendor Notification Date.	20-Mar-2012
Product.	Mi-Token Enterprise Edition & API Edition
Platform.	All
Affected versions.	Mi-Token Enterprise 4.3.5 and earlier Mi-Token API Edition 4.3.5 and earlier
Severity Rating.	Medium
Impact.	Brute-force Security bypass
Attack Vector.	Remote with authentication
Solution Status.	Vendor patch
CVE reference.	CVE- Not yet assigned

Summary.

The Mi-Token Two-Factor Authentication (2FA) system before version (4.3.6) does not implement rate-limiting or lockout on One-Time-Password (OTP) verification attempts.

This can allow brute-forcing of the second factor, reducing the system strength to that of password-based logins.

The required one-time password or token could be bypassed by brute-force in around 30 minutes in the deployment tested.

Mitigating Factors.

- Valid credentials are required, only second factor (OTP or token) is brute-forced
- Excludes Mi-Token Banking Edition
- Systems integrated with Mi-Token which implement their own rate-limiting or lockout could mitigate this vulnerability

Details.

Given valid domain credentials (e.g. captured by a key-logger), Sense of Security were able to gain access to a Juniper SSL VPN solution protected by the Mi-token 2FA scheme. It was possible to guess the token in a short amount of time (around 30 minutes on average) due to a combination of flaws in the combined authentication scheme.

The observed token values were configured at 6 digits long. A-priori, the probability of guessing a valid OTP token is about 1 in 1 million. Furthermore, the solution (Juniper SSL VPN) blocks the client's IP for about 10 minutes after a relatively small number of invalid requests (approximately 5). However:

1) To account for time differences between the server and the 2FA device, several previous and future token values will be accepted by the server. At least 5 'previous' and future token values were accepted by the SSL VPN server tested.
    - This reduced the effort by a factor of 10.
2) The system accepted arbitrary digits before the valid token value. For example, XXXXXX123456 will result in a successful login, where X is any digit, if 123456 is the valid token. Furthermore, 123456XXXXXX is also valid. This means that TWO guesses can be attempted per HTTP POST request to the server.
    - This again halved the brute-force effort.
3) The Juniper SSL VPN's IP-based blocking could be circumvented by using a large number of different IP addresses. This could be achieved either by having a large net-block at your disposal or using many proxies. Sense of Security used several hundred publicly listed proxies for testing and verified that there was no global account lockout, no matter how many authentication requests were submitted.
    - This allowed bypass of request blocking

Accounting for these weaknesses, each HTTP POST to the server has a probability of success around 1 in 50,000. Since unlimited authentication attempts can be submitted, the only remaining parameter which affects cracking speed is the number of requests per second which can be issued to the server. In our testing, we managed at least 20 requests per second.

Considering each authentication attempt as an independent event (token values were chosen randomly for each request), the odds of n incorrect authentication attempts in a row are 49999/50000 ^ n.

This means the token can be guessed correctly:

With 50% probability in: 34,657 attempts (~30 minutes at 20 reqs/sec)

With 90% probability in: 115,128 attempts (~90 minutes at 20 reqs/sec)

Proof of Concept.

Exploit code is available to Sense of Security customers.

Solution.

Customers running Mi-Token or Mi-Token Enterprise versions older than 4.3.6 should contact Mi-Token support for an update.

Mi-Token has released a policy module implementing locking or throttling, which has been natively incorporated into the latest Mi-Token version.

Discovered by.

Blair Strang 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-13-002.pdf

Other Sense of Security advisories can be found at:
http://www.senseofsecurity.com.au/research/it-security-advisories.php