Sense of Security	Authorisation. Jason Edelstein
	Release date. 25 October 2018.

Sense of Security – Security Advisory – SOS-18-003.

Inteset Secure Lockdown Standard Edition – Privilege Escalation and Insecure Cryptographic Storage.

25 October 2018.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 25 October 2018.

Inteset Secure Lockdown Standard Edition – Privilege Escalation and Insecure Cryptographic Storage Security Advisory - SOS-18-003

Release Date.	25-Oct-2018
Vendor Notification Date.	23-Feb-2018
Product.	Inteset Secure Lockdown Standard Edition
Platform.	Tested on Microsoft Windows 7, 8.1 and 10
Affected versions.	Tested versions v2.00.160 -> v2.00.196
Severity Rating.	High
Impact.	Privilege escalation Security bypass
Attack Vector.	From local system
Solution Status.	Currently no solution
CVE reference.	CVE - Not yet assigned

Details.

The Inteset Secure Lockdown desktop application allows the use of the deprecated SHA-1 hash function to store the Inteset administrator's password in the Windows registry. The hash can be found at the following registry location:

`HKEY_CURRENT_USER\Software\Inteset\SecureLockdown_v2\Password`

The above key is configured to be read and can be written to by the logged in user by design. This allows an attacker to view or edit the registry while the application is running and replace the stored hash with a self-generated known plain-text hash value. More recent versions of the application use a stronger PKCS1 RSA function to store the password, though the stored value is still susceptible to being replaced with an attacker-known value to escalate permissions.

Once the hash has been replaced the user can open Inteset using the 'alt + shift + s' key combination and enter the newly configured password to take control of the locked down system.

Furthermore, there are multiple ways to bypass the Lockdown functionality features in Inteset. For example, as part of the 'System Lockdown / Local Level' configuration options, an administrator can select 'No Network Shares' and 'No Local Drives'. An attacker with an all options enabled Inteset deployment, only needs to gain access to a file dialogue box and use a Universal Naming Convention (UNC) path, such as '`\\localhost\c$`', to give the user access to both the local disk and the local network share.

To obtain administrative shell level access to the system, an attacker can for example, execute the following command to gain a PowerShell prompt from a file open dialogue box:

```
'\\localhost\c$\Windows\System32\WindowsPowerShell\v1.0\powershell.exe'
```

Proof of Concept.

Once a shell has been gained on the system as per the above example, the following PowerShell command can be executed to set the Inteset Administrator password to 'Oliver9!' and take control of the locked down system:

```
PS> Set-ItemProperty -Path
"HKCU:\Software\Inteset\SecureLockdown_v2" -Name Password -
Value B8EF8772E5241A1E5441B2DC8650B487588EA423
```

The above method will bypass any Inteset lockdown configuration, including the restriction to edit the registry.

Solution.

No vendor supplied solution has been offered.

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 cyber security advisor to many of the country's largest organisations.

	Authorisation. Jason Edelstein
	Release date. 25 October 2018.

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: https://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-18-003.pdf

Other Sense of Security advisories can be found at:

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