Cisco DoS due to SMI

CPU usage goes high for no reason

Gianrico Fichera vs 1.0 - May 8, 2018

Cisco Smart Install vulnerability

The Smart Install feature permit zero-config installation for some Cisco devices with IOS or IOS-XR. If that feature is enabled there could be an external abuse that could lead a remote attacker to get access.

In this example we have a Cisco Switch 3750 attacked from an outside net.

Here is how to check if the SMI feature in activated (by default in this case):

```
itesys_test#show vstack config | inc Role
Role: Client (SmartInstall enabled)
```

I noticed the attack because the system CPU utilization was too high:
In normal condition the CPU should be 5/10%. As you can see the processor resources are used by the *SMI IBC* process without apparent reason.

```
itesys_test#sh process cpu sorted
CPU utilization for five seconds: 52%/0%; one minute: 55%; five minutes: 60%
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
221   371808903    49800965       7465 41.82% 47.15% 53.02%   0 SMI IBC server p
```

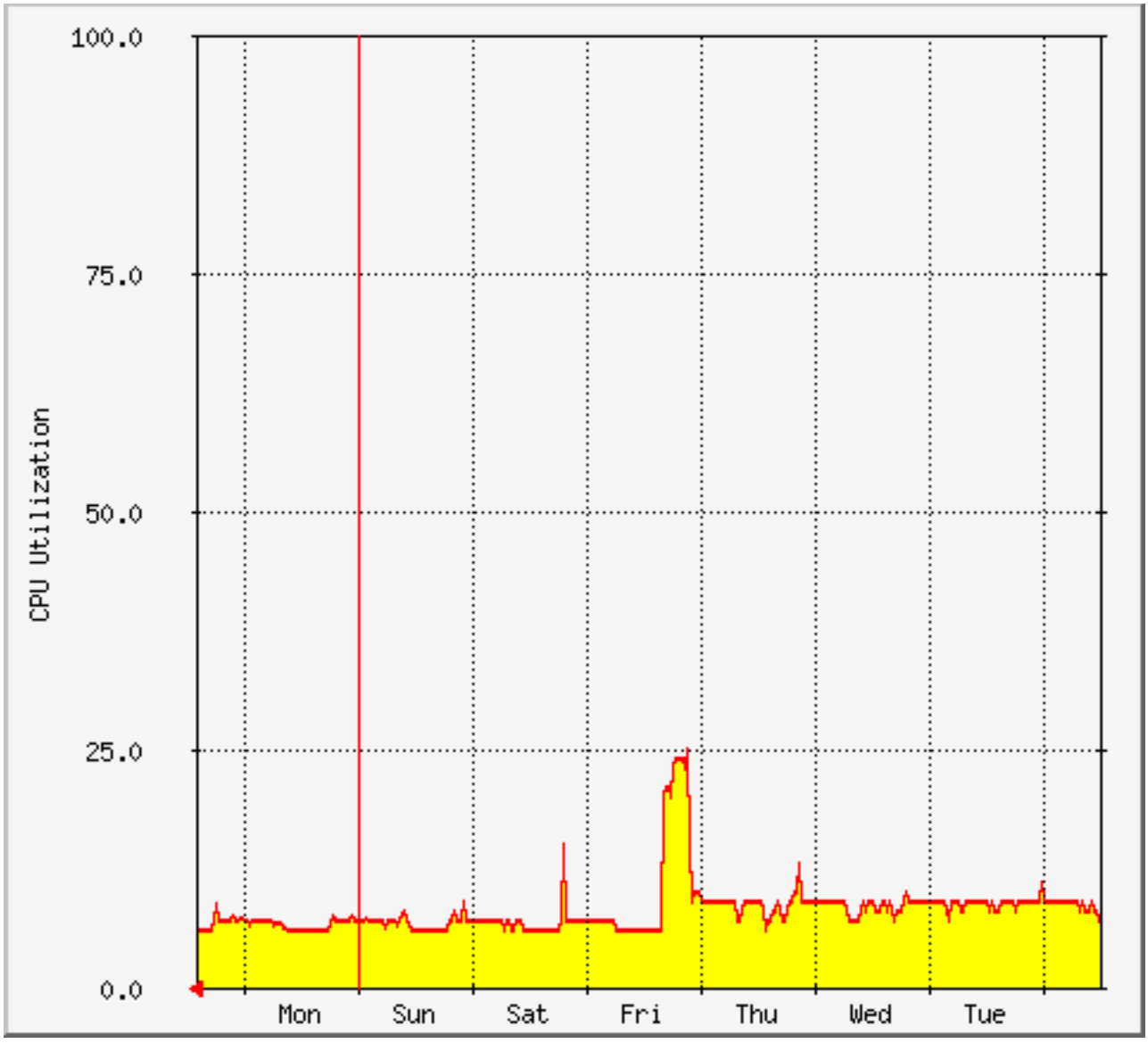
So I disabled the Smart Install feature:

```
itesys_test#conf t
itesys_test(config)#no vstack
itesys_test(config)#exit

itesys_test#show vstack config | inc Role
Role: Client (SmartInstall disabled)
```

After disabled SMI the processor goes to 5/10% and we resolved the issue. For more information you can check the Cisco Advisory cisco-sa-20170214-smi.

As general advise, especially in case of Cisco switch devices, you should always monitor the CPU load: this should be low. If there are spikes it could means that too many packets are pinned to the CPU and this should not happen with devices that use hardware TCAM for move packets. For example on Friday in this Cisco switch something happen:



Copyright and General Advice Disclaimer

Tutti i marchi riportati appartengono ai legittimi proprietari; questo documento non e' sponsorizzato o sottoscritto dalle società eventualmente citate. L'autore di questo documento non si assume nessuna responsabilità e non da nessuna garanzia riguardante l'accuratezza o la completezza delle informazioni presenti nonché da conseguenze sull'uso delle informazioni presenti.

This material is not sponsored by, endorsed by, or affiliated with anyone. All trademarks are trademarks of their respective owners. I tried to ensure the accuracy and completeness of the contents of this document, but I cannot offer any undertaking or guarantee, either expressly or implicitly regarding how correct, complete or up to date the contents of this document are. I reserve the right to supplement this document at any time or to change or delete any information contained or views expressed.