Cisco® IOS® and IOS XE® Software Smart Install Denial of Service Vulnerability

Date: May 23, 2018

Overview:

The affected network switches are susceptible to a Denial of Service vulnerability. Cisco's Cyber Security Advisory (cisco-sa-20180328-smi) provides the details of the vulnerability, including the specific Internetworking Operating System (IOS) and all affected product on Cisco's website at

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi

Environment:

Part Number	Description
117T6409P023A	2960X ROOT BRIDGE SWITCH STACK
117T6409P023B	2960X ROOT BRIDGE SWITCH 4-STACK
117T6409P024A	2960X ROOT BRIDGE SWITCH STACK
117T6409P024B	2960X ROOT BRIDGE SWITCH 4-STACK
117T6409P025A	2960X EDGE SWITCH STACKED PAIR
117T6409P025B	2960X EDGE SWITCH STACKED PAIR
117T6409P025C	2960X EDGE SWITCH STACKED PAIR
117T6409P025D	2960X EDGE SWITCH STACKED PAIR
117T6409P025E	2960X EDGE SWITCH STACKED PAIR
117T6409P025F	2960X SINGLE SWITCH WITH STACK
117T6409P027A	2960X XDH SWITCH FOR NETWORKST
117T6409P030A	2960X ROOT BRIDGE SWITCH STACK
117T6409P030B	2960X ROOT BRIDGE SWITCH STACK
117T6409P030AAAB	2960X ROOT BRIDGE SWITCH STACK
117T6409P030BAAB	2960X ROOT BRIDGE SWITCH STACK
117T6409P031AAAB	2960X EDGE SWITCH NOT STACKED
117T6409P032AAAB	2960X EDGE SWITCH NOT STACKED
117T6409P032BAAB	2960X EDGE SWITCH NOT STACKED
117T6409P033AAAB	2960X EDGE SWITCH NOT STACKED
117T6409P033BAAB	2960X EDGE SWITCH NOT STACKED

117T6409P040AAAA	CISCO IE 2000 8 PORT EDGE SWITCH
117T6409P041AAAA	IE2000 8 PORT EDGE SWITCH
117T6409P041BAAA	IE2000 8 PORT EDGE SWITCH
117T6409P042AAAA	IE2000 8 PORT EDGE SWITCH
117T6409P042BAAA	IE2000 8 PORT EDGE SWITCH
117T6409P043AAAA	CISCO IE 2000 16 PORT EDGE SWITCH
117T6409P044AAAA	IE2000 16 PORT EDGE SWITCH
117T6409P044BAAA	IE2000 16 PORT EDGE SWITCH
117T6409P045AAAA	IE2000 16 PORT EDGE SWITCH
117T6409P045BAAA	IE2000 16 PORT EDGE SWITCH

Recommendations:

It is recommended to disable the Smart Install client feature on all affected switches installed at a customer plant as part of the GE scope of supply.

To determine if a device is configured with the Smart Install feature enabled, use the **show vstack config** privileged EXEC command on the Smart Install client.

An output of **Role: Clientand Oper Mode: Enabled or Role: Client (SmartInstall enabled**) from the **show vstack** config command confirms that the feature is enabled on the device.

The following examples show the output of the **show vstack config** command on Cisco Catalyst switches that are configured as Smart Install clients:

```
switch1# show vstack

config Role: Client (SmartInstall enabled)

.

.

.

switch2# show vstack config

Capability: Client

Oper Mode: Enabled

Role: Client
```

To disable the Smart Install feature, issue the "**no vstack**" command in privilege EXEC mode on the switch configuration console.

The command takes effect immediately but must be persisted by saving the configuration to the device.

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0025957

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.