Software Advisory Notice

Dear Cisco Customer,

Cisco has identified the following software issue with the release that you have selected. This may affect your use of this software. Please review the Software Advisory notice here to determine if the issue applies to your environment. You may proceed to download this software if you have no concerns with the issue described.

For more comprehensive information about what is included in this software, refer to the Cisco software Release Notes, available from the Product Selector tool. From this page, select the product in which you are interested. The Release Notes are under "General Information" on the product page.

Affected Software and Replacement Solution for CSCvp77466		
Software Type	**Software Affected Versions:**	**Software Solution Fixed Software versions:**
Cisco Tetration	Based on running Kernel version. For more information, see the advisories from the OS distributors that are listed under "Issue Description."	Patch your operating system as described in the "Workaround" section.

Reason for Advisory

Due to a bug in the Linux kernel's IPSet code, a Linux system might panic when concurrent IPSet commands are issued.

Affected Software

This issue affects the Cisco Tetration enforcement agent that is running on an unpatched kernel version that has enforcement enabled. For more information, see the advisories listed under "Issue Description."

Issue Description

When the Tetration Enforcement Agent enforces or re-enforces a policy on a Linux machine, the agent executes several ipset commands. If an administrator runs an "ipset list" or an "ipset save" command simultaneously, there is a slight chance that the kernel could panic due to a bug in the kernel's ip_set code.

Instances of this bug have been reported for different Linux distributions, as described in the following Linux bugs:

- https://access.redhat.com/solutions/3520061
- https://bugs.centos.org/view.php?id=13767

- https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1793753

Workaround

Contact your OS vendor and install the recommended patches to address the issue.
Do not run the "ipset save" or "ipset list" commands on an unpatched host that is running the enforcement agent with enforcement enabled.

Upstream bug references:

- https://github.com/torvalds/linux/commit/596cf3fe5854fe2b1703b0466ed6bf9cfb83c91e
- https://github.com/torvalds/linux/commit/e5173418ac597cebe9f7a39adf10be470000b518