Software Advisory Notice

Dear Cisco Customer,

Cisco has identified software issues that may affect your use of software you have selected. Review this Software Advisory notice to determine if the issues apply to your environment.

If these issues apply, perform one of the workarounds described in the second table below. When a fix is available, upgrade or apply the patch release specified in the "Software solution – Fixed software versions" column in the first table below.

Note: Cisco Tetration is now known as Cisco Secure Workload.

Affected Software and Replacement Solution for CSCvx74789		
Bug ID	**Software Affected Versions**	**Software Solution Fixed Software versions**
CSCvx74789	Cisco Tetration versions: 3.5.1.1 3.5.1.2	Cisco Tetration patch release newer than 3.5.1.2 Cisco Secure Workload release 3.6 or newer

Reason for Advisory:

This software advisory addresses one software issue.

Affected Software:

Cisco Tetration Software Release versions mentioned in the above table.

Bug CSCvx74789

Issue Description	Windows Defender with Advanced Security firewall was disabled on Windows workloads when Tetration enforcement agent version 3.4.1.x or older was installed with enforcement settings disabled in the agent config profile. After upgrading to or installing Tetration Enforcement Agent version 3.5.1.1, Windows Defender with Advanced Security is now enabled regardless of the enforcement setting in the agent config profile. Depending on the existing rules in the firewall, this might cause network interruption. This issue does not affect Windows deep visibility agents.
Conditions	This issue occurs when the following conditions are met: • Upgrade to or install enforcement agent 3.5.1.1 with enforcement disabled in the agent config profile • Windows firewall is OFF for any profile and there is no associated GPO profile enablement settings for Windows Defender with Advanced Security

Workaround	**Option 1:** If 3.4.1.x or earlier version of Tetration enforcement agent is installed on the host, disable auto upgrade in the agent config profile for the Windows hosts before upgrading to Tetration software release 3.5.1.1. Leave enforcement agents on existing version until a patch with fix is available. This issue does not affect deep visibility agents, so those can be upgraded. **Option 2:** If version 3.4.1.x or earlier of a Tetration enforcement agent is installed on the host, create GPO (domain or local) to explicitly disable all Firewall profiles before upgrading to Tetration version 3.5.1.1. A GPO setting takes precedence over the agent setting. This option is recommended only if no policies are enforced on the windows workload. **Option 3**: If new Tetration agent 3.5.1.1 is being installed on the workloads, create GPO (domain or local) to explicitly disable all Firewall profiles before installing Tetration Agent version 3.5.1.1. A GPO setting takes precedence over the agent setting.

For information about what is included in each software release, see the Release Notes for the release, available from https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html.