Dear Cisco Customer,

Cisco engineering has identified the following software issues with the release that you have selected that may affect your use of this software. Please review the Software Advisory notice here to determine if the issues apply to your environment.

The affected Firepower software is no longer available.

Reason for Advisory:
This software advisory addresses one software issue.

Affected Software and Replacement Solution for CSCvk67239		
Software Type	**Software Affected**	**Software Solution**
Firepower Threat Defense	**Version:** • Version 6.2.3.5 build 52 • ASA 9.9(2.16)- 9.9(2.22) • ASA 9.8(3.9) and later **Affected Images:** • Cisco_FTD_SSP_Patch-6.2.3.5-52.sh.REL.tar • Cisco_FTD_SSP_FP2K_Patch-6.2.3.5-52.sh.REL.tar • Cisco_FTD_Patch-6.2.3.5-52.sh.REL.tar	**Version:** Version 6.2.3.6 **Replacement Images:** TBD

CSCvk67239
FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"

Affected Platforms:
- ASA 5500-X Series with FTD (ASA 5506-X series, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X)
- Firepower 2100 Series with FTD (2110, 2120, 2130, 2140)
- Firepower 4100 Series with FTD (4110, 4120, 4140, 4150)
- Firepower 9300 with FTD
- ISA 3000 with FTD
- FTDv

Symptom:

ASA Firewalls and Firepower Threat Defense devices may traceback and reload when the state of the unit in a Failover pair or multi-unit cluster changes. For example, when moving from ACTIVE to STANDBY or STANDBY to ACTIVE, or as it joins/leaves a cluster. The problem also occurs during software upgrade.

Conditions:
To encounter the problem, the following conditions must be met:

1) Syslogging to an off-box syslog host must be configured, using the UDP logging protocol
2) FTD device running Firepower 6.2.3.5
   Note: ASA firewalls running ASA 9.9(2.16)-9.9(2.22) or ASA 9.8(3.9) and later are also affected. Versions outside of these ranges are not affected by the problem
3) A unit must leave and then join the high availability (cluster or failover) and this might happen during a software upgrade

The problem occurs in cluster and failover high availability setups, and can be triggered during a high-availability upgrade. For example, during the process of upgrading from 6.2.3.5 to a later version such as 6.2.3.6, after one unit successfully upgrades to 6.2.3.6, another unit still running 6.2.3.5 might encounter the problem as it is upgrading and attempting to re-join the cluster.

Workaround:
Disable the external UDP syslogging on the affected device. You can configure TCP logging instead of UDP logging.

To disable UDP logging on FTD from the FMC UI, see the Configure Syslog Logging for FTD Devices chapter of the Firepower Management Center Configuration Guide.

To disable Cisco ASA logging, see the Logging chapter of the Cisco ASA Series General Options CLI Configuration Guide.

> ***NOTE***:
> If you configure TCP logging, appropriately configure the `logging permit-hostdown` feature for your environment. If this feature is not present in your firewall configuration, and your TCP syslog server is not reachable by the firewall for any reason, the firewall drops new connections. Refer to the configuration links above for ASA or FTD to ensure this is set as desired.

After you disable UDP syslogging, you can successfully upgrade to Version 6.2.3.6.