

山西省互联网网络安全预警信息通报

山西省通信管理局

主办：国家计算机网络应急技术处理协调中心山西分中心 2020年10月31日

关于 Cisco Firepower 2100 系列拒绝服务漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了 Cisco Firepower 2100 系列拒绝服务漏洞（CNVD-2020-59747）。攻击者可利用该漏洞，通过受影响的设备发送格式错误的 SSL TLS 消息。成功利用该漏洞可以使设备重新加载，从而导致 DoS 状态。

一、漏洞情况分析

Cisco Firepower Threat Defense（FTD）是美国思科（Cisco）公司的一套提供下一代防火墙服务的统一软件。

Cisco Firepower Threat Defense 存在安全漏洞。该漏洞源于对特定 SSL TLS 消息的某些字段的输入验证不当造成的。攻击者可利用该漏洞，通过受影响的设备发送格式错误

的 SSL TLS 消息。成功利用该漏洞可以使设备重新加载，从而导致 DoS 状态。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

Cisco Cisco Firepower 2100 系列

三、处置措施

厂商已发布了漏洞修复程序，请及时关注更新：

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ssl-dcrpt-dos-RYEKX4yy>

参考链接：

<https://nvd.nist.gov/vuln/detail/CVE-2020-3562>