The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
10/29/2021

SUBJECT:
A Vulnerability in Cisco Adaptive Security Appliance and Firepower Threat Defense Could Allow for Security Bypass

OVERVIEW:
A vulnerability has been discovered in Cisco Adaptive Security Appliance and Firepower Threat Defense, which could allow attackers to bypass security mechanisms on the system. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to bypass security mechanisms on the targeted host.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Cisco Adaptive Security Appliance (ASA) Software 9.7 and earlier
- Cisco Adaptive Security Appliance (ASA) Software prior to 9.8.4.40
- Cisco Adaptive Security Appliance (ASA) Software prior to 9.12.4.25
- Cisco Adaptive Security Appliance (ASA) Software prior to 9.14.3.1
- Cisco Adaptive Security Appliance (ASA) Software prior to 9.15.1.17
- Cisco Adaptive Security Appliance (ASA) Software prior to 9.16.1.28
- Cisco Adaptive Security Appliance (ASA) Software 9.9, 9.10, and 9.13
- Cisco Firepower Threat Defense (FTD) Software 6.3 and earlier
- Cisco Firepower Threat Defense (FTD) Software prior to 6.4.0.13
- Cisco Firepower Threat Defense (FTD) Software prior to 6.6.5
- Cisco Firepower Threat Defense (FTD) Software prior to 6.7.0.3
- Cisco Firepower Threat Defense (FTD) Software prior to 7.0.1
- Cisco Firepower Threat Defense (FTD) Software prior to 7.0.1
- Cisco Firepower Threat Defense (FTD) Software 6.5

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Cisco Adaptive Security Appliance and Firepower Threat Defense, which could allow attackers to bypass security mechanisms on the system. The vulnerability is the result of a design error in the identity-based firewall (IDFW) rule processing feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software, which could allow an unauthenticated, remote attacker to bypass security protections (CVE-2021- 34787). Attackers may be able to exploit this issue by sending a specially crafted network request to an affected device.

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY

CVE:
https://www.cve.org/CVERecord?id=CVE-2021-34787

TLP: WHITE
https://www.cisa.gov/tlp