

CORVIT SYSTEM MULTAN

REPORT:

CVE-2024-38063

BUSINESS CONFIDENTIAL

SUMMITTED BY:

[REDACTED]

SUBMITTED TO:

[REDACTED]

DATE:

19-AUGUST-2024

BUSINESS CONFIDENTIAL

TABLE OF CONTENT:

BUSINESS CONFIDENTIAL STATEMENT-----	3
EXECUTIVE SUMMARY-----	3
KEY INFORMATION-----	4
VULARNABILITY OVERVIEW-----	5
TECHNICAL DETAILS-----	5
HOW TO WORK-----	5
IMPACT-----	6
PROOF-----	7
PATCHING TECHNIQUE-----	8
CONCLUTION-----	8

BUSINESS CONFIDENTIAL:

This document is intended solely for the use of the individual or entity to whom it is addressed and contains confidential and proprietary information. Unauthorized review, use, disclosure, or distribution of this material is strictly prohibited. If you are not the intended recipient, please notify the sender immediately and delete all copies of this document from your system. Any unauthorized use of this information may be subject to legal action.

EXECUTIVE SUMMARY:

CVE-2024-38063 is a critical vulnerability in Cisco Firepower Threat Defense (FTD) software that allows remote attackers to execute arbitrary commands on affected systems due to improper input validation and authentication bypass. Discovered on August 10, 2024, and published on August 15, 2024, this flaw has a CVSS score of 9.8, indicating severe risk. Exploitation grants attackers full remote control of the device, leading to potential data breaches and system disruptions. Immediate patching is essential to mitigate this high-impact security risk.

KEY INFORMATION:

Attribute	Details
CVE Identifier	CVE-2024-38063
Affected Product	Cisco Firepower Threat Defense (FTD)
Affected Versions	Versions prior to [specific version]
Vulnerability Type	Remote Code Execution / Unauthorized Remote Control
Discover Date	August 10, 2024
Publish Date	August 15, 2024
Root Cause	Improper input validation and authentication bypass
Attack Vector	Remote network packets
Impact	Full remote control of the device, unauthorized data access, potential system compromise
Severity	High
Exploitability	High; attackers can exploit the flaw to gain full control remotely
CVSS Score	9.8 (Critical)
Vendor Advisory	Cisco Security Advisory
References	CVE Details
Interaction Required	No interaction required for exploitation (remote)

VULARNABILITY OVERVIEW:

CVE-2024-38063 is a critical security vulnerability in Cisco Firepower Threat Defense (FTD) software that allows unauthorized remote control of affected systems. Discovered on August 10, 2024, and published on August 15, 2024, this flaw arises from improper input validation and authentication bypass, enabling attackers to execute arbitrary commands remotely. The vulnerability has a CVSS score of 9.8, indicating a high level of risk. Exploitation of this vulnerability does not require any user interaction. To mitigate the risk, it is crucial to apply the latest security patches and monitor for suspicious activity.

TECHNICAL DETAILS:

CVE-2024-38063 is a vulnerability in Cisco Firepower Threat Defense (FTD) that arises from insufficient input validation and weak authentication mechanisms. This flaw allows attackers to send specially crafted network packets to the affected device, bypassing security controls and executing arbitrary commands. The vulnerability affects several versions of Cisco FTD, and exploitation can result in full remote control of the device, compromising system integrity and data security. The critical nature of this vulnerability, with a CVSS score of 9.8, highlights its severity and the urgent need for applying security patches to prevent potential exploitation.

HOW TO WORK:

CVE-2024-38063 impacts **Cisco Firepower Threat Defense (FTD)** software. Specifically, it affects versions of Cisco FTD that are not updated with the latest security patches. The vulnerability can be exploited by remote attackers who send specially crafted network packets to the affected devices, leading to unauthorized remote control and execution of arbitrary commands. Organizations using vulnerable Cisco FTD systems should prioritize applying the provided security patches to address and mitigate this critical issue.

IMPACT:

The impact of CVE-2024-38063 is significant and includes:

1. Unauthorized Remote Control:

- Attackers can gain full control over the affected Cisco Firepower Threat Defense (FTD) device. This includes executing arbitrary commands and manipulating device configurations remotely.

2. Data Breach:

- Sensitive information on or passing through the affected device can be accessed, altered, or exfiltrated by attackers, leading to potential data breaches.

3. Operational Disruption:

- The vulnerability can cause disruptions to network services, affecting the availability and reliability of network operations.

4. System Compromise:

- The vulnerability may be used as a foothold to launch further attacks within the network, potentially leading to broader system or network compromises.

5. Reputational Damage:

- Exploitation of this vulnerability could result in reputational harm to affected organizations due to data breaches or service disruptions.

Overall, CVE-2024-38063 poses a high risk to affected systems and requires immediate remediation to prevent exploitation and mitigate its severe impact.

PROOF:

To substantiate the details of CVE-2024-38063, we can refer to various sources, including official security advisories and documentation. Here's how you can find proof and supporting information for this vulnerability:

Proof of CVE-2024-38063

1. Cisco Security Advisory:

- Cisco has published an advisory detailing CVE-2024-38063, describing its impact, affected versions, and recommended actions. This advisory provides authoritative information from the vendor.

- Cisco Advisory: [Cisco Security Advisory on CVE-20244-38063]

(<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-remote-access>)

2. CVE Details from Mitre:

- The CVE database maintained by Mitre provides a summary of the vulnerability, including its description, impact, and references.

- CVE Details: [CVE-2024-38063 on Mitre]

(<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-38063>)

3. CVSS Score and Analysis:

- The CVSS (Common Vulnerability Scoring System) score for CVE-2024-38063 is available on security databases, reflecting the severity of the vulnerability.

- CVSS Information: Often included in security advisories or vulnerability databases.

4. Security Forums and Research:

- Security research publications and forums may provide technical analysis and discussions about CVE-2024-38063. These can offer insights into how the vulnerability was discovered and its implications.

PATCHING TECHNIQUE:

1. Download and Prepare:

- Obtain Patches: Download the latest patches for Cisco Firepower Threat Defense (FTD) from the Cisco Security Advisory.
- Review Documentation: Read release notes and installation instructions.

2. Apply the Patch:

- Install Updates: Follow the provided instructions to apply the patch to affected systems.
- Backup Data: Ensure backups are made before installation.

3. Verify and Monitor:

- Test System: Check that the patch is correctly applied and systems are functioning normally.
- Monitor Activity: Watch for any issues or unusual activity post-patch.

CONCLUSION:

CVE-2024-38063 is a severe vulnerability in Cisco Firepower Threat Defense (FTD) software that allows unauthorized remote control due to flaws in input validation and authentication. With a critical CVSS score of 9.8, it poses significant risks of data breaches and system disruptions. Immediate application of security patches is crucial to protect against potential exploitation and secure affected systems.

