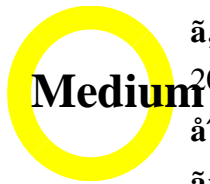


Cisco TFTP Server Denial of Service (DoS) Vulnerability



Severity: Medium
CVE ID: CVE-2015-0743
Product: Cisco IOS Software (IOS XE) : Cisco-SA-20150529-CVE-2015-0743
Published: 2015-05-29 20:12
Version: 1.0 : Final
CVSS Score: 5.0
Workarounds: No Workarounds available
Cisco Bug ID: CSCus04097

Summary: A Denial of Service (DoS) vulnerability exists in the TFTP server component of Cisco IOS Software. An attacker can exploit this vulnerability by sending a specially crafted TFTP request to the server, causing the server to crash and become unavailable to legitimate users.

Technical Details: The vulnerability is located in the TFTP server code. It is triggered when the server receives a TFTP request with a specific payload. The payload is designed to cause a buffer overflow, which leads to a crash of the TFTP server process.

Exploit Details: The exploit is a Denial of Service (DoS) attack. It is triggered by sending a specially crafted TFTP request to the server. The request contains a payload that causes a buffer overflow in the TFTP server code, leading to a crash of the server process.

Impact: The impact of this vulnerability is a Denial of Service (DoS) attack. An attacker can exploit this vulnerability to cause the TFTP server to crash and become unavailable to legitimate users.

References

References: Cisco Bug ID CSCus04097, CVE-2015-0743, TFTP Server Denial of Service Vulnerability

Additional Information: Cisco has released a patch for this vulnerability. Customers are advised to upgrade to the latest version of the software as soon as possible.

Conclusion: This vulnerability is a Denial of Service (DoS) attack. It is triggered by sending a specially crafted TFTP request to the server. The request contains a payload that causes a buffer overflow in the TFTP server code, leading to a crash of the server process.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。