

GRUB2

High



CVE-2020-10713 : cisco-sa-grub2-code-exec-xLePCAPY

[CVE-2020-10713](#)

2020-08-04 23:00

2020-08-10 15:49

1.1 : Interim

No workarounds available

Cisco ID :

There is a hole in the Unified Bootloader version 2 (GRUB2) that can be used to execute arbitrary code on the system.

Summary

There is a hole in the Unified Bootloader version 2 (GRUB2) that can be used to execute arbitrary code on the system.

This vulnerability affects Unified Bootloader version 2 (GRUB2) versions 2.04-rc1 through 2.04-rc3. It allows an attacker to execute arbitrary code on the system.

The vulnerability is located in the `grub2` package. It is caused by a buffer overflow in the `grub2` code. An attacker can exploit this vulnerability by sending a specially crafted request to the system.

Unified Extensible Firmware Interface (UEFI)

The vulnerability is located in the `grub2` package. It is caused by a buffer overflow in the `grub2` code. An attacker can exploit this vulnerability by sending a specially crafted request to the system.

This vulnerability affects Unified Bootloader version 2 (GRUB2) versions 2.04-rc1 through 2.04-rc3.

The vulnerability is caused by a buffer overflow in the `grub2` code. An attacker can exploit this vulnerability by sending a specially crafted request to the system.

Cisco Bug

This vulnerability is tracked as [CVE-2020-10713](#) in the Cisco Security Center for Cybersecurity.

For more information, please refer to the [Cisco Security Advisory](#).

For more information, please refer to the [Cisco Security Advisory](#).

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-grub2-code-exec-xLePCAPY>

References

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。