



CVE-2020-17407

Published on: 10/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:30 PM UTC

CVE-2020-17407

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Bullet-lte](#) from [Microhardcorp](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Microhard Bullet-LTE prior to v1.2.0-r1112. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of authentication headers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-10596.

CVE-2020-17407 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Microhard - Bullet-LTE** version prior to v1.2.0-r1112

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

ZDI-20-1206 | Zero Day Initiative

Tags

Third Party Advisory

VDB Entry

www.zerodayinitiative.com

text/html

Link

 MISC www.zerodayinitiative.com/advisories/ZDI-20-1206/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Microhardcorp	Bullet-lte	-	All	All	All
Hardware 	Microhardcorp	Bullet-lte	-	All	All	All
Operating System	Microhardcorp	Bullet-lte Firmware	All	All	All	All
Operating System	Microhardcorp	Bullet-lte Firmware	All	All	All	All
cpe:2.3:h:microhardcorp:bullet-lte:-:*:*:*:*:*:						
cpe:2.3:h:microhardcorp:bullet-lte:-:*:*:*:*:*:						
cpe:2.3:o:microhardcorp:bullet-lte_firmware:*:*:*:*:*:						
cpe:2.3:o:microhardcorp:bullet-lte_firmware:*:*:*:*:*:						

Discovery Credit

Ricky "HeadlessZeke" Lawshae

← Previous ID

Next ID →