ADVISORY DETAILS

January 29th, 2021

Fuji Electric V-Server Lite VPR File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

ZDI-21-099
ZDI-CAN-11669

CVE ID

CVE-2021-22641

CVSS SCORE

7.8, (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

AFFECTED VENDORS

Fuji Electric

AFFECTED PRODUCTS

V-Server Lite

VULNERABILITY DETAILS

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Fuji Electric V-Server Lite. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the parsing of VPR files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.

ADDITIONAL DETAILS

Fuji Electric has issued an update to correct this vulnerability. More details can be found at:
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01

DISCLOSURE TIMELINE

2020-09-02 - Vulnerability reported to vendor
2021-01-29 - Coordinated public release of advisory
2021-06-29 - Advisory Updated

CREDIT

khangkito - Tran Van Khang of VinCSS (Member of Vingroup)

‹ BACK TO ADVISORIES