summtime Update README.md ... on Nov 9, 2020 History

..

README.md 2 years ago

README.md

CVE-2020-28250: Cellinx NVT Webserver Root Privilege Escalation

I. VULNERABILITY

Cellinx NVT Web Server 5.0.0.014b.test 2019-09-05 allows a remote user to run commands as root via SetFileContent.cgi because authentication is on the client side.

II. CVE REFERENCE

CVE-2020-28250

III. VENDOR

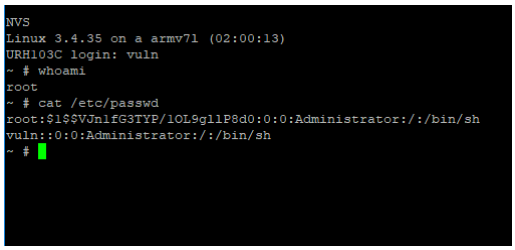
Cellinx Systems, Ltd. (https://sites.google.com/view/cellinx-systems-eng)

IV. TIMELINE

2020/01/22 - Vulnerability discovered

V. DESCRIPTION

This vulnerability is caused by the lack of access control in the NVT Webserver which can manage their products through web page. NVT Web enables only an administrator to access 'Setting' button which is written in Javascript. The attacker can change HTTP requests and responses because authentication is on the client side. 'GetFileContent.cgi' reads the contents of the file. Since the web server process is running with root privileges, it can read sensitive information such as /etc/passwd. The attacker can also create a root account on the server without password by using 'SetFileContent.cgi' like below.



VI. REFERENCES

CWE-264 Permissions, Privileges, and Access Controls