Fujitsu Eternus Storage DX200 S4 Broken Authentication

2020.11.26

Seccops (https://cxsecurity.com/author/Seccops/1/) (TR)

Risk: Medium | Local: Yes | Remote: Yes

CVE: CVE-2020-29127 (https://cxsecurity.com/cveshow/CVE-2020-29127/) | CWE: CWE-287 (https://cxsecurity.com/cwe/CWE-287)

CVSS Base Score: **10/10**
Exploitability Subscore: **10/10**
Attack complexity: **Low**
Confidentiality impact: **Complete**
Availability impact: **Complete**

Impact Subscore: **10/10**
Exploit range: **Remote**
Authentication: **No required**
Integrity impact: **Complete**

```
# Title: Fujitsu Eternus Storage DX200 S4 Broken Authentication
# Author: Seccops (https://seccops.com)
# Vendor Homepage: https://www.fujitsu.com/global/products/computing/storage/disk/eternus-dx/
# Version: Fujitsu Eternus Storage DX200 S4 devices through 2020-11-25
# Classifications: OWASP: A2:2017-Broken Authentication, CWEs: CWE-287 & CWE-1028
# CVE: CVE-2020-29127


=== Description ===

An issue was discovered on Fujitsu Eternus Storage DX200 S4 devices through 2020-11-25. After logging into the portal as a root user (usi
ng any web browser), the portal can be accessed with root privileges when the URI "cgi-bin/csp?cspid={XXXXXXXXXX}&csppage=cgi_PgOverview&
csplang=en" is visited from a different web browser.

After logging into the portal with a "root" user using any web browser, the portal can be accessed with "root" privileges when the link
(http://eternus/cgi-bin/csp?cspid={XXXXXXXXXX}&csppage=cgi_PgOverview&csplang=en) formed is entered from a different web browser.

Example: https://imgur.com/a/kuhCi04
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020110215)

Tr | Lul

Vote for this issue: 2 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)