CVE-2021-39285

CVE-2021-39285 Versa Director Cross Site Scripting Vulnerability

A **XSS** Vulnerability exists in **Versa Director Release: 16.1R2 Build: S8.** An attacker can use the administration web interface URL to create a XSS based attack.

Vulnerability Information

Vulnerability Type:

Reflected Cross-site Scripting (XSS) occur when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself; it is non-persistent and only impacts users who open a maliciously crafted link or third-party web page. The attack string is included as part of the crafted URI or HTTP parameters, improperly processed by the application, and returned to the victim.

Vulnerability Root Cause:

When a web application is vulnerable to this type of attack, it will pass unvalidated input sent through requests back to the client. The common modus operandi of the attack includes a design step, in which the attacker creates and tests an offending URI, a social engineering step, in which she convinces her victims to load this URI on their browsers, and the eventual execution of the offending code using the victim's browser.

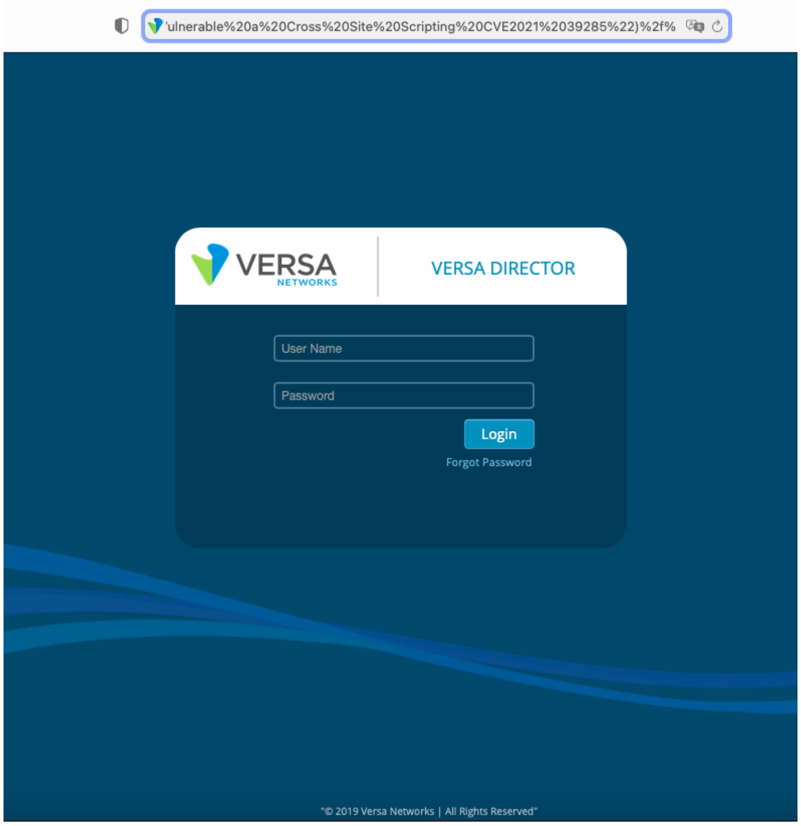
One of the primary difficulties in preventing XSS vulnerabilities is proper character encoding. In some cases, the web server or the web application could not be filtering some encodings of characters, so, for example, the web application might filter out <script>, but might not filter %3cscript%3e which simply includes another encoding of tags.

Vulnerability Impact:

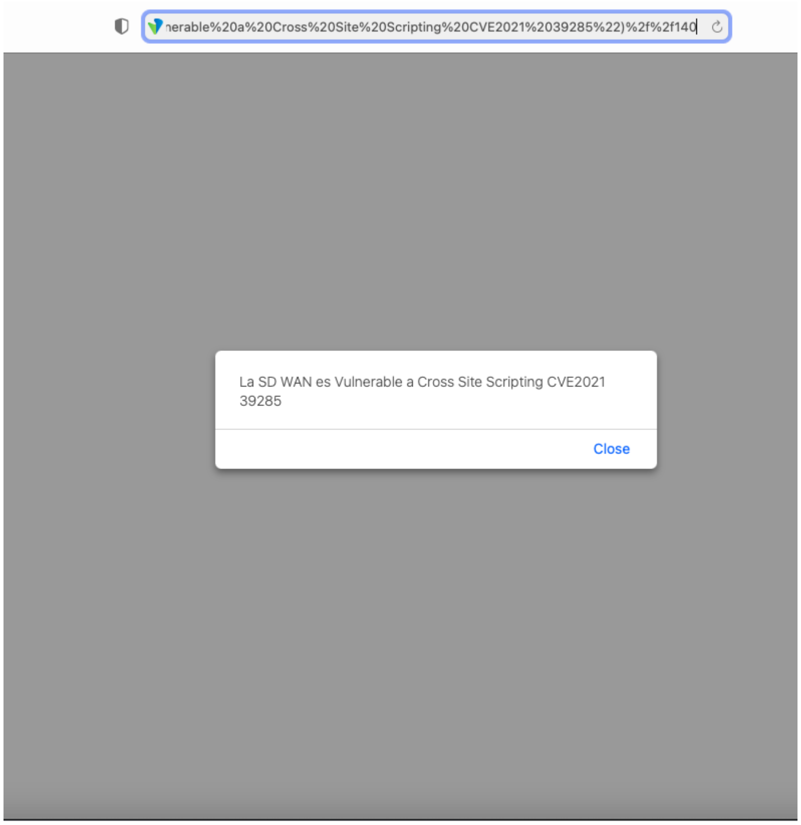
Commonly the attacker's code is written in the JavaScript language, but other scripting languages are also used, e.g., ActionScript and VBScript. Attackers typically leverage these vulnerabilities to *install key loggers, steal victim cookies, perform clipboard theft, and change the content of the page* (e.g., download links).

PoC

Proof of Concept: A proof of concept can be executed by crafting a URL using the Versa Director Web URL. The XSS Attack must be included in the specially crafted URL.


'ulnerable%20a%20Cross%20Site%20Scripting%20CVE2021%2039285%22)%2f%
VERSA
NETWORKS
VERSA DIRECTOR
User Name
Password
Login
Forgot Password
"© 2019 Versa Networks | All Rights Reserved"

After the exploit is executed the XSS message will appear.


ıerable%20a%20Cross%20Site%20Scripting%20CVE2021%2039285%22)%2f%2f140
Close

La SD WAN es Vulnerable a Cross Site Scripting CVE2021 39285

Recommendations

The recommendation is to apply the necessary updates recommended by vendor to remediate this vulnerability.

Disclosure Information

Vulnerability discovered by Pablo Barrera. Vendor notified in August 2019.