Rob_NES Follow
Aug 10 · 3 min read · Listen

CVE-2022–38168: Avaya Scopia Pathfinder Broken Access Control

Update 11/2/22: I was finally issued a CVE for this!

CVE-2022–38168: **UNSUPPORTED WHEN ASSIGNED** Broken Access Control in User Authentication in Avaya Scopia Pathfinder 10 and 20 PTS version 8.3.7.0.4 allows remote unauthenticated attackers to bypass the login page, access sensitive information, and reset user passwords via URL modification.

I was recently doing a pentest on a company and found a Scopia Pathfinder from the company Avaya. This is a device used for video-conferencing between organizations. I was doing some enumeration and manual testing and found quite the little issue; just my changing the URL, you can bypass the login form and get to the password reset page for any registered user. For full context, I contacted Avaya about this and they said:

> *Thank you for providing the details of your findings. After going through Avaya documentation, we have confirmed that the Product mentioned Avaya Scopia Pathfinder has reached end of manufacture support in March 11, 2020. We will not be providing any further support or issuing CVEs for any findings related to this product.*

I understand the product is no longer supported, but there are organizations and industries that don't necessarily upgrade to the latest and greatest, and felt it should at least be out there. Regarding the writ

> *Once again, thank you for reporting your findings through Avaya's Ethical Disclosure process. We hope to hear from you in the future if you have more findings!*

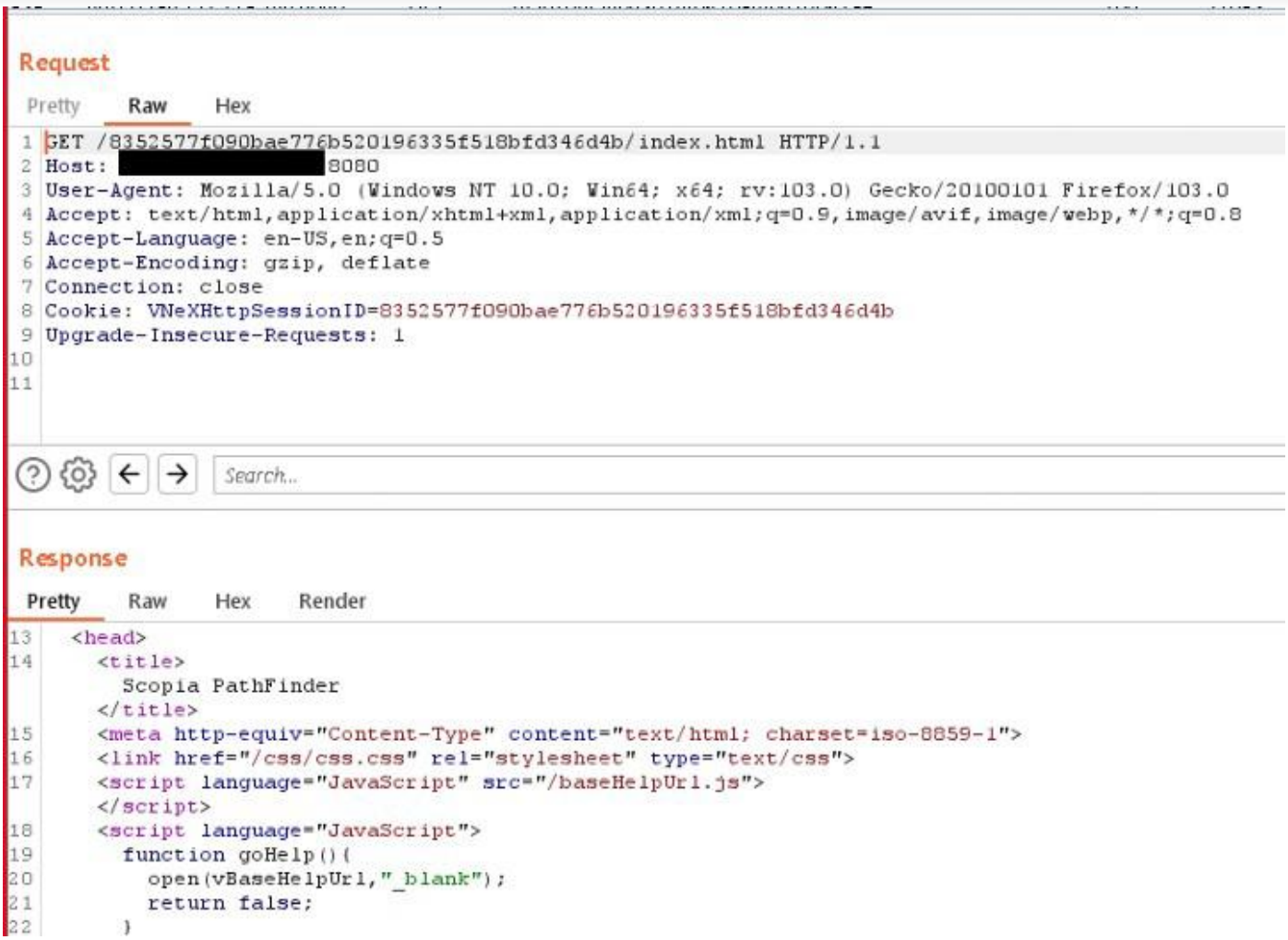
So it goes like this...

Avaya Scopia Pathfinder

Version: 8.3.7.0.4
DATE RELEASED: Jan 2, 2017

Broken Access Control

Access the website running the software. When accessed, the site will assign you a session token using the cookie VNeXHttpSessionID. This will also redirect you to a page on the site with that session ID as the path.



The request and response for the login form in Burp.

The request in Burp Suite, with the response redirecting to “ClientStatus”.

The new “ClientStatus” page shows an unknown user being logged in, with access to the various menus and settings inside the site, without ever having to enter any login information.

The logged in page with the various menus in the browser.

When the Users tab is clicked, the User List is blank. However, inside the HTML for the page, there is a link (hidden due to no users being listed) for a UserEdit page.

The blank Users page and the “UserEdit” code in the Developer Tools.

The page showing the prompt for the Password Change.

From this, you can also access the Settings tab, accessible from the “blank” user after the authentication bypass and the System Info, indicating the version installed on the device.

Very simple, but effective. Be aware!