Multiple vulnerabilities in Syncovery for Linux

JOBS

Multiple vulnerabilities were found in Syncovery for Linux backup tool. We've reported them to the software vendor and they were fixed in version 9.48j. Vulnerable are all versions **below v9.48j** including all versions of branch 8.

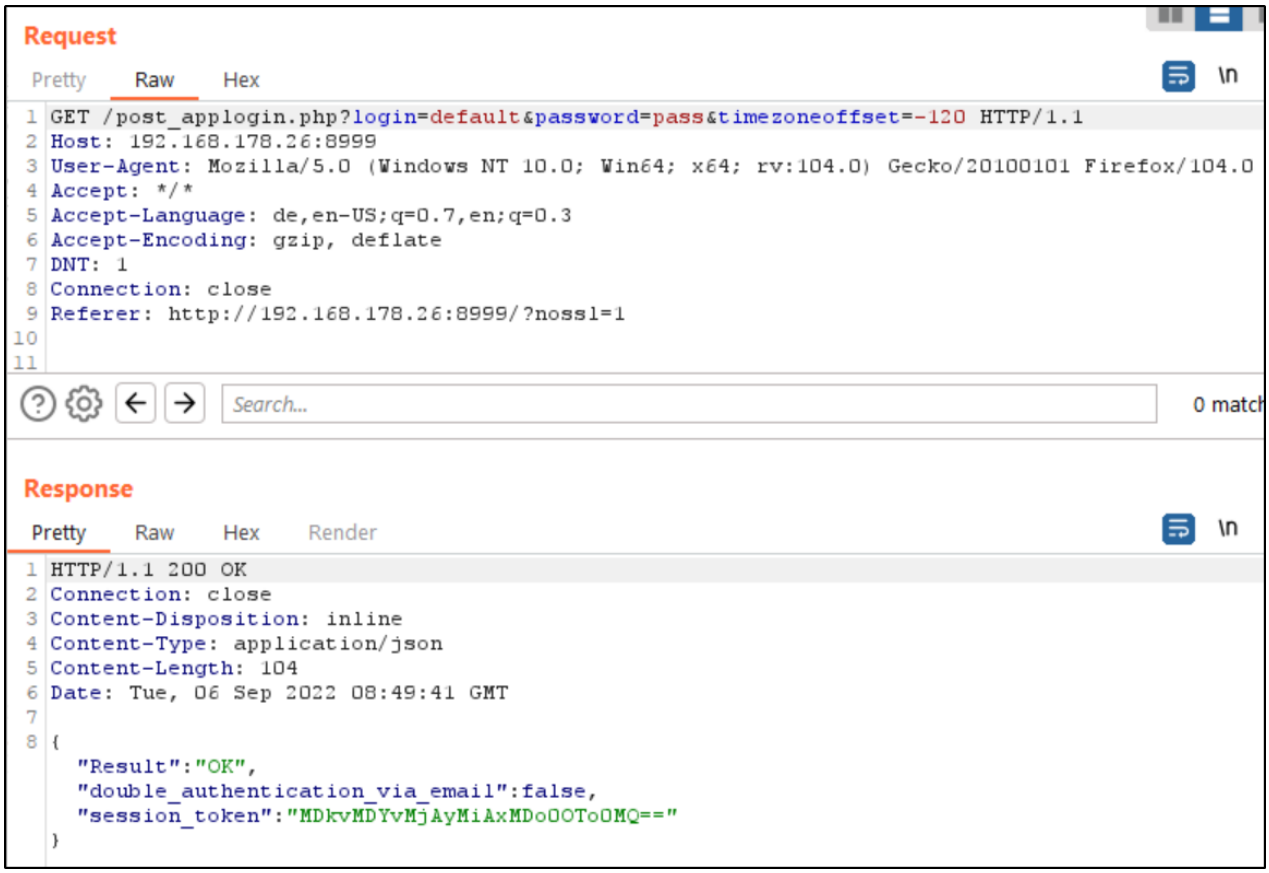
Insecure Session Token Creation (CVE-2022-36536)

Description

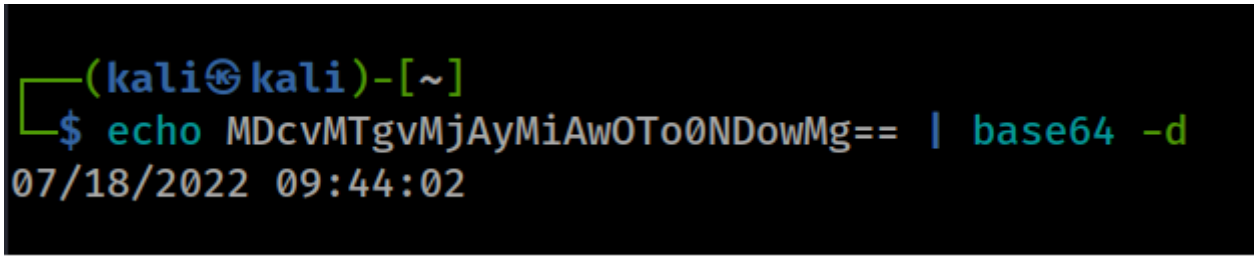
Up to Syncovery v9.48j session tokens are generated in an insecure manner:

> base64(MM/dd/yyyy HH:mm:ss)

The following screenshot shows the session token after a successful login:



The token can be decoded easily to verify, that the date and time was used for token creation:



Affected Component

Login (post_applogin.php)

Attack Type

Remote

Impact Escalation of Privileges

True

Attack Vectors

Attackers can easily brute-force valid session tokens with a simple script. On success, the attacker has full administrative access to the web GUI.

Reference

https://www.syncovery.com/detailed-version-history/

Discoverer

Jan Rude (mgm security partners)

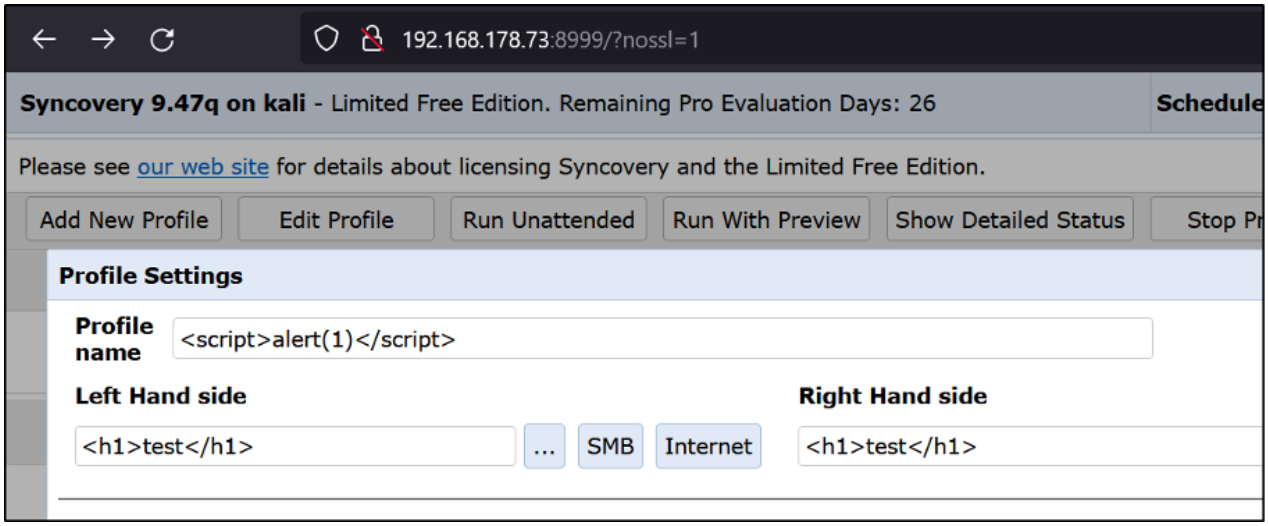
Stored Cross-Site Scripting vulnerabilities (CVE-2022-36533)

Description

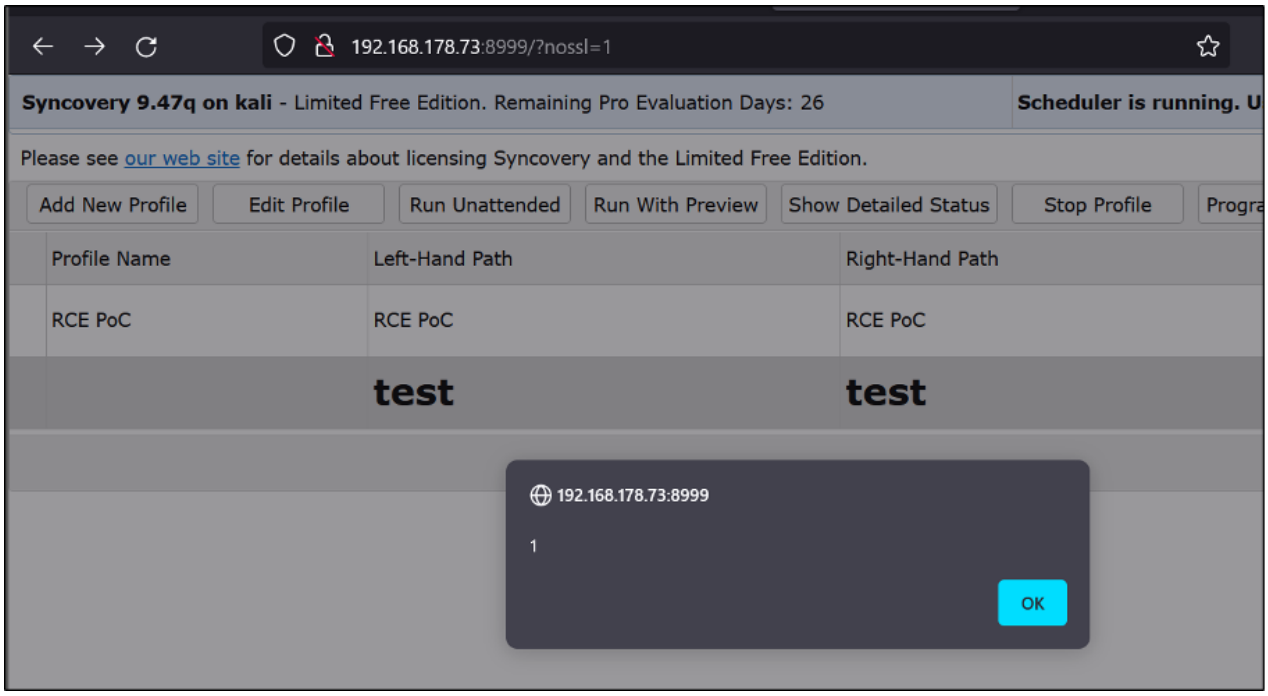
Syncovery up to version 9.48j is vulnerable to stored Cross-site Scripting due to missing output encoding of the profile settings.

JOBS

A user can store arbitrary JavaScript code in the profile settings that is executed each time the profiles are viewed.



The h1 tags in „LeftPath“ and „RightPath“ are interpreted as HTML and the JavaScript code gets executed as well:



Affected Component

Parameters *ProfileName*, *OriginalProfileName*, *LeftPath* and *RightPath* of post_profilesettings.php

JOBS

Attack Type

Remote

Impact Code Execution

True

Attack Vectors

To exploit the vulnerability, an attacker needs access to the application.

Reference

https://www.syncovery.com/detailed-version-history/

Discoverer

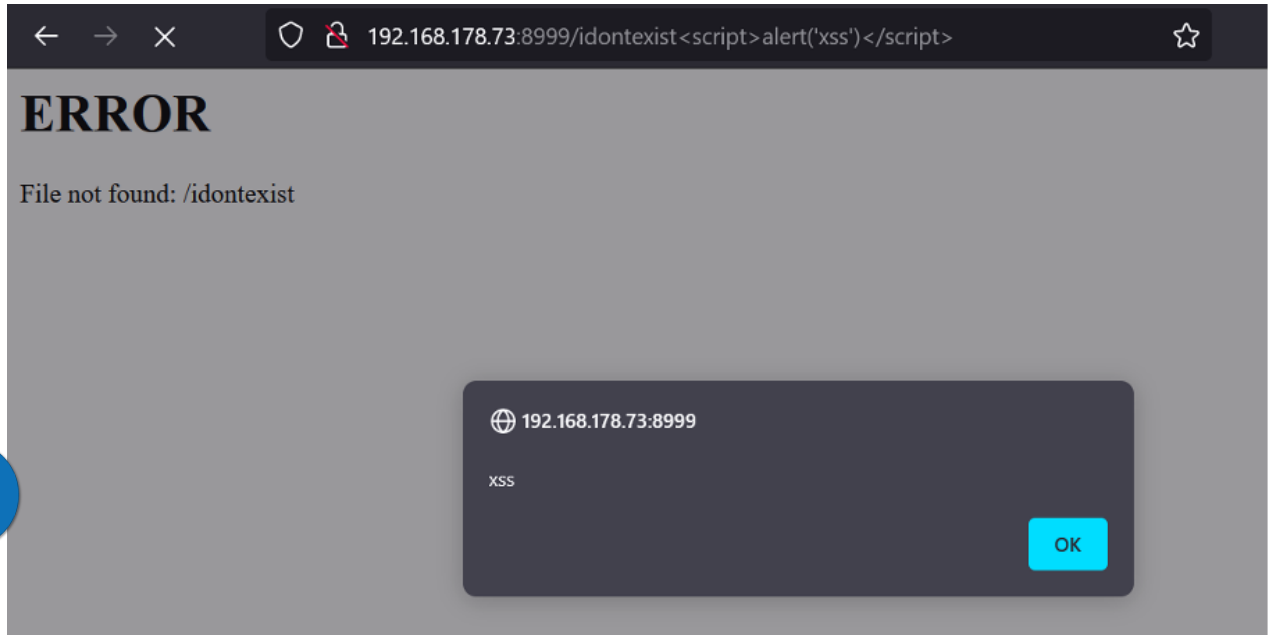
Jan Rude (mgm security partners)

Reflected Cross-Site Scripting vulnerabilities (CVE-2022-36533)

Description

Syncovery up to version 9.48j is vulnerable to reflected Cross-site Scripting due to missing output encoding in error pages and status pages.

The reflected XSS can be exploited by crafting a malicious link to an error message:



Affected Component

Default error page

Parameter profile of status.php

Attack Type

Remote

Impact Code Execution

True

Attack Vectors

To exploit the vulnerability, an attacker needs to craft a malicious link.

Reference

https://www.syncovery.com/detailed-version-history/

Discoverer

Jan Rude (mgm security partners)

Authenticated Remote Code Execution (CVE-2022-36534)

Description

Syncovery allows users to execute a command or script before/after running a profile.

Since it is possible to inject arbitrary commands an authenticated attacker can get root access to the host by inserting a crafted payload. This results in a complete compromise of the server running Syncovery.

JOBS

Example: Insertion of a PHP reverse shell as „Before“ command. Executing this command will open a new connection (reverse shell) to the attacker machine.

The attacker is listening on the port 4444 until the Syncovery host connects to the attacker machine. Since the software is running with root privileges by default, the attacker has root access to the host.

Affected Component

‘Job_ExecuteBefore’ and ‘Job_ExecuteAfter’ parameter in post_profilesettings.php.

Attack Type

Remote

Impact Code Execution

True

Attack Vectors

To exploit the vulnerability, an attacker needs access to the application.

Reference

https://www.syncovery.com/detailed-version-history/

Discoverer

Jan Rude (mgm security partners)

Timeline

- 2022/07/05 – Identification of the vulnerabilites
- 2022/07/08 – Informing the vendor about the vulnerabilities
- 2022/07/18 – CVE Request
- 2022/08/31 – Release of new Syncovery version which fixes the vulnerabilities
- 2022/09/06 – Publication