NSA workflow application Emissary vulnerable to malicious takeover

Adam Bannister 07 April 2021 at 14:28 UTC
Updated: 07 April 2021 at 15:16 UTC

Vulnerabilities | Open Source Software | Research

Users urged to update their systems after disclosure of serious vulnerabilities

Emissary, an open source, peer-to-peer (P2P) workflow engine developed by the US National Security Agency (NSA), contains vulnerabilities that attackers could chain to take over Emissary instances.

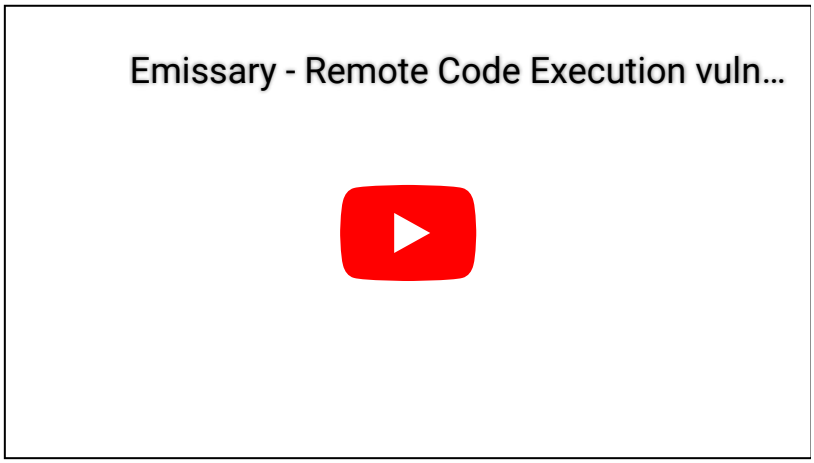
Users have been urged to update their systems after the discovery of five security flaws in the Java web application, which runs in a multi-tiered P2P network of computer resources.

In a blog post published on Monday (April 5), security researchers from Swiss infosec outfit SonarSource demonstrated how an attacker could mount a cross-site request forgery (CSRF) attack against a logged-in user to exploit a code injection vulnerability and achieve remote code execution (RCE).

Read more of the latest open source security news

They also combined arbitrary file disclosure and reflected cross-site scripting (XSS) flaws to read arbitrary files from the Emissary server.

Once the XSS payload is executed in the victim's browser, the file disclosure vulnerability could be exploited to read administrator credentials and relay them to an attacker-controlled server – resulting in a "quick and easy" server compromise demonstrated in the video below:



XSS and arbitrary file disclosure

The Emissary XSS flaw was found in a `DocumentAction` error response message generated when a requested document was not found, resulting in user input being reflected without output encoding.

An attacker could therefore craft a malicious link that, if clicked by an authenticated victim, passes a payload that executes JavaScript in the browser, explained SonarSource researcher Dennis Brinkrolf.

RELATED NSA advises US security supply chain on replacing deprecated encryption protocols

Latest Posts

Deserialized web security roundup
Fortinet, Citrix bugs; another Uber breach; hacking NFTs at Black Hat

Critical IP spoofing bug patched in Cacti
'Not that hard to execute if attacker has access to a monitoring platform running Cacti'

Casting a SpEL
Akamai WAF bypassed via Spring Boot to trigger RCE

The file disclosure flaw was found in a feature showing configuration files. The user-controlled HTTP `GET` variable `CONFIG_PARAM` was received from the query string, and the `configName` variable was not sanitized and could contain any file path.

A path traversal attack that injects character sequences such as `../` would therefore enable a malicious user to access authentication files on Emissary's HTTP Digest Authentication function, which by default has administrator credentials for only a single user.

Remote takeover

Found in a console feature used to evaluate Ruby code, the code injection bug arises from the absence of CSRF tokens.

Brinkrolf demonstrated how if the user-controlled post parameter `CONSOLE_COMMAND` mirrors the string eval then an attacker-controlled post variable, `CONSOLE_COMMAND_STRING`, is received and passed to the function `evalAndWait()` from the `RubyConsole` class.

The vulnerable `eval()` function then receives a Ruby expression as the first parameter controllable by an attacker, who can therefore execute arbitrary Ruby code through the browser of a logged-in administrator.

SonarSource researchers also discovered authenticated file delete and file upload vulnerabilities.

Disclosure timeline

The vulnerabilities were found in Emissary version 5.9.0.

The researchers initiated contact with Emissary's maintainers on September 24, 2020, and sent them an advisory on October 16. Version 5.11.0, which addressed the RCE issue, was then issued on December 15.

After being notified of the remaining vulnerabilities on January 7, Emissary maintainers then released version 6.1 on March 2.

However, on March 5 SonarSource informed maintainers that the CSRF and path traversal problems remained unpatched.

The Daily Swig has asked the maintainers about a timeline for final patches – we will update this article if and when we hear back.

RELATED LocalStack zero-day vulnerabilities chained to achieve remote takeover of local instances

Vulnerabilities | Open Source Software | Research | Hacking News | Hacking Techniques | CSRF | Path Traversal | RCE | XSS | Java | Authentication | Privacy | Organizations | Network Security | US | Switzerland | North America | Europe | Browsers

Adam Bannister

@Ad_Nauseum74

Related stories

Deserialized web security roundup

Fortinet, Citrix bugs; another Uber breach; hacking NFTs at Black Hat

16 December 2022

Critical IP spoofing bug patched in Cacti

15 December 2022

Casting a SpEL

Akamai WAF bypassed via Spring Boot to trigger RCE

14 December 2022

Cloud flaws brought to the fore as bug bounty vulnerabilities hit 65k in 2022

13 December 2022