Multiple vulnerabilities in Pandora FMS could trigger remote execution attack

Charlie Osborne 25 September 2020 at 14:15 UTC
Updated: 07 October 2020 at 14:45 UTC

RCE Vulnerabilities SQL Injection

Researchers find four now-patched flaws risking the security of enterprise networks

Critical vulnerabilities lurking in Pandora FMS could have led to the full compromise of enterprise infrastructure and networks.

Developed by Ártica ST, Pandora FMS is an open source solution that provides an interface for monitoring network connections, app management, event alerts, and both agent and agentless monitoring for Windows, Linux, Unix, and Android systems.

On September 22, SonarSource cybersecurity researcher Dennis Brinkrolf explained the potential impact of four vulnerabilities recently discovered in Pandora FMS version 742. All flaws have since been patched.

In a blog post, Brinkrolf said the vulnerabilities included a pre-auth SQL injection bug, a pre-auth PHAR deserialization flaw, a lowest privileged-user remote file inclusion coding error, and a cross-site request forgery (CSRF) issue.

According to the researcher, the pre-auth SQL injection is particularly severe, as this can lead to "a complete takeover of the application and put further network systems at risk".

"[The vulnerability] can be remotely exploited without any access privileges and enables an attacker to completely bypass the administrator authentication," Brinkrolf explained. "This enables, in the end, [the execution of] arbitrary code on the system."

Brinkrolf added that no prior knowledge of a target system or specific configuration is required to launch an attack.

Attack vectors

During a SonarSource analysis of the software, the company found several Pandora FMS instances that were open and exposed to the internet – one potential entryway into a target system. If a victim is able to reach a Pandora FMS installation via their browser, visiting a crafted, malicious website can also trigger an attack.

The researcher says that the root cause of the vulnerability existed in Pandora FMS' PHP source code.

Specifically, a failure to properly sanitize user input and the use of a wrapper which allows access to `$_GET` or `$_POST` variables directly could be exploited by attackers to launch an SQL injection attack.

Pandora FMS internal functions can dynamically build SQL queries based on table names and conditions. If supplied by an attacker, these variables can end up in a SQL database without proper sanitization.

With the right payload, threat actors can then impersonate administrators with full access privileges. Due to the severity of the vulnerability, the researchers have chosen not to disclose the "exact" method of exploit.

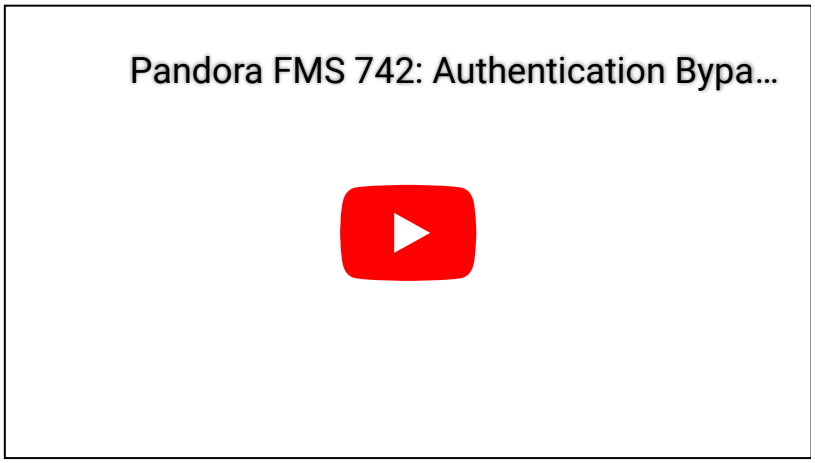
However, the "quick and easy" method to take over a server has been demonstrated in the proof-of-concept (PoC) video below:

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



Another attack vector is the deserialization of arbitrary objects via SQL injection, as long as a login bypass is achieved – a security flaw raised in previous advisories.

"We reported all issues responsibly to the affected vendor who released a security patch, version 743, immediately," Brinkrolf commented. "We would like to thank the Pandora FMS team."

Read more of the latest cybersecurity vulnerability news

The vulnerabilities were patched in the January Pandora FMS release, version 743 (PDF). The current build is 749, which includes fixes for unrelated cross-site scripting (XSS) security flaws.

Pandora replied to a request for comment from *The Daily Swig*, simply confirming that they had fixed the flaws in version 743 and that further details can be found in Brinkrolf's blog post.

READ MORE Action View: XSS bug discovered in popular Ruby Gem

RCE | Vulnerabilities | SQL Injection | Cyber-attacks | Hacking Techniques | Network Security | Open Source Software | Hacking News

Charlie Osborne

@SecurityCharlie

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