Date: Tue, 12 Jan 2021 13:59:59 +0100
From: Marcus Meissner <meissner@...e.de>
To: OSS Security List <oss-security@...ts.openwall.com>
Subject: Security issues in hawk2 and crmsh

Hi folks,

We have received reports of 2 security issues for hawk and crmsh. These
hawk and crmsh projects refer to distros@ for their disclosure work.

These issues were reported to SUSE by Vincent Berg of Anvil Ventures.

1. Remote unauthenticated shell injection into the Hawk webserver

   Hawk is a High Availability specific webconsole with its own webserver.

   The Hawk webserver versions 2.2 up to now have a shell code injection
   issue via the "hawk_remember_me_id" cookie.

   It can be triggered from 2 places, via /login (with login_from_cookie) and /logout
   interfaces.

   The cookie value is passed unquoted and unfiltered from ruby to a
   shell command as commandline argument. (Using %[shellcommand] pattern.)

   As hawk is running as "hauser" usually, this allows unauthenticated
   remote attackers to gain access to the "hauser" account.

   Introduced by https://github.com/ClusterLabs/hawk/commit/a939a099c6abdac383fbaede5e8655853222c887#diff-5349b200e8dc7ea82818115aa0aa1522

   We have received CVE-2020-35458 from Mitre for this issue.

   Our team did a fix that does not use an subshell to invoke the command, patch is attached.

2. Local root privilege escalation via hawk and crmsh shell code injection

   crmsh is a commandline shell utility to query or configure a HA cluster.

   The Hawk webconsole contains a "setuid root" helper tool called "hawk_invoke", which
   allows hawk to call some root functionality in "crmsh".

   hawk_invoke allows calls from "hauser" or "vagrant" users only.

   hawk_invoke has a whitelist of "crmsh" commandline options, but does not do any
   filtering or blocking of stdin.

   The "crm history" sub-command is whitelisted by hawk_invoke.

   It opens its own sub-shell with various commands, one of them is "session create SESSION"
   This subcommand will create a directory "SESSION" by calling:

                if utils.pipe_cmd_nosudo("mkdir -p %s" % session_dir) != 0:

   which again does not filter the input.

   This allows local privilege escalation from "hauser" or "vagrant" to root.

   We have received CVE-2020-35459 from Mitre for this issue.

   Currently we will fix only the unsafe mkdir and add ; to the blacklist filtering, a patch is attached.

Due to shortness of time we did not yet do a full (re)audit of crmsh and hawk, we are currently working on that.

The whole hawk_invoke setuid root setup also needs a full redesign.

Ciao, Marcus

View attachment "hawk2-CVE-2020-35458.patch**" of type "**text/x-patch**" (1974 bytes)**

View attachment "crmsh-CVE-2020-35459.patch**" of type "**text/x-patch**" (3341 bytes)**