

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



SMA Technologies Patches Critical Security Issue in Workload Automation Solution

By [Ionut Arghire](#) on June 22, 2022

Share

Tweet

推荐 0



A critical vulnerability in the SMA Technologies OpCon UNIX agent results in the same SSH key being deployed with all installations.

Aimed at financial institutions and insurance firms, OpCon is a cross-platform process automation and orchestration solution that can be used for the management of workloads across business-critical operations.

Tracked as CVE-2022-2154, the issue results in the same SSH key being delivered on every installation and subsequent updates, the CERT Coordination Center (CERT/CC) at Carnegie Mellon University explains in an [advisory](#).

The SSH public key is added to the root account's *authorized_keys* file during the agent's installation, and the entry remains there even after the OpCon software has been removed.

The installation files also include a corresponding, unencrypted private key named "sma_id_rsa."

"An attacker with access to the private key included with the OpCon UNIX agent installation files can gain SSH access as root on affected systems," CERT/CC noted.

The bug impacts version 21.2 and earlier of the OpCon UNIX agent. SMA Technologies, which was informed of the security issue in March, told CERT/CC that it has already updated the version 21.2

package to remove the vulnerability.

“We have analyzed the reported vulnerability and have created a utility that can be applied to remove the vulnerability from affected systems. The utility should be run as soon as possible to all UNIX/Linux/AIX systems using the OpCon UNIX agent to prevent any potential exploitation,” the company said.

SMA says its [removal tool](#) checks the *authorized_keys* file for the vulnerable SSH key and moves it from there, while informing the user that it has found and removed it. It also removes the vulnerable public and private keys from other folders where they might reside.

The issue can also be addressed by manually removing the SSH key entry from root's *authorized_keys* file, CERT/CC notes.

Related: [Cisco Patches Critical Vulnerability in Email Security Appliance](#)

Related: ['Follina' Vulnerability Exploited to Deliver Qbot, AsyncRAT, Other Malware](#)

Related: [Critical U-Boot Vulnerability Allows Rooting of Embedded Systems](#)

Share

Tweet

推荐 0



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Chinese APT 'Bronze Starlight' Uses Ransomware to Disguise Cyberespionage](#)

[MCG Health Faces Lawsuit Over Data Breach Impacting 1.1 Million Individuals](#)

[SMA Technologies Patches Critical Security Issue in Workload Automation Solution](#)

[Delivery Firm Yodel Scrambling to Restore Operations Following Cyberattack](#)

[Google Patches 14 Vulnerabilities With Release of Chrome 103](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[2022 Singapore/APAC ICS Cyber Security Conference\]](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

Tags:

[NEWS & INDUSTRY](#)

[Vulnerabilities](#)

Search

Get the Daily Briefing

BRIEFING

Business Email Address

Subscribe

