Cisco sneaks another hardcoded secret root backdoor into video surveillance kit

Who watches the watchers? Anybody who has the login

By Richard Chirgwin 22 Reg comments SHARE ▼

It's a giant city-destroying bug - geddit, bug? Software bug?

If you run Cisco's video surveillance kit, hop over to Switchzilla's support site and download the latest version of its management software.

Late last week, the networking giant admitted that its Cisco Video Surveillance Manager Appliance has an undocumented root account with static hard-coded credentials.

Reading between the lines, someone created the “secret” account during product development, and forgot about it: “The root account of

the affected software was not disabled before Cisco installed the software on the vulnerable platforms.”

Because the hard-coded account has administrator-grade root privileges, an attacker able to reach the equipment over the network can do anything once they've logged in.

From its CVE-2018-15427 advisory: "A vulnerability in Cisco Video Surveillance Manager (VSM) Software running on certain Cisco Connected Safety and Security Unified Computing System (UCS) platforms could allow an unauthenticated, remote attacker to log in to an affected system by using the root account, which has default, static user credentials.

“This vulnerability affects Cisco Video Surveillance Manager (VSM) Software Releases 7.10, 7.11, and 7.11.1 if the software was preinstalled by Cisco and is running on the following Cisco Connected Safety and Security Unified Computing System (UCS) platforms: CPS-UCSM4-1RU-K9; CPS-UCSM4-2RU-K9; KIN-UCSM5-1RU-K9; KIN-UCSM5-2RU-K9.”

Products in the clear are releases earlier than VSM Software 7.9; later versions if they were installed as upgrades to VSM 7.9; or VSM Software VMWare's ESXi platform. ®