Pulse Secure - April 20, 2021

The Pulse Secure team recently discovered that a limited number of customers have experienced evidence of exploit behavior on their Pulse Connect Secure (PCS) appliances. We are sharing information about the investigation and our actions through several communications channels in the best interests of our customers and the greater security community.

The team has been working proactively with leading forensic experts and industry groups, including Mandiant/FireEye, CISA and Stroz Friedberg, among others, to investigate and respond to the exploit behavior.

We have discovered four issues, the bulk of which involve three vulnerabilities that were patched in 2019 and 2020: Security Advisory SA44101 (CVE-2019-11510), Security Advisory SA44588 (CVE-2020-8243) and Security Advisory SA44601 (CVE-2020-8260). We strongly recommend that customers review the advisories and follow the recommended guidance, including changing all passwords in the environment if impacted.

There is a new issue, discovered this month, that impacted a very limited number of customers. The team worked quickly to provide mitigations directly to the limited number of impacted customers that remediates the risk to their system. We will be releasing a software update in early May. Visit Security Advisory SA44784 (CVE-2021-22893) for more information.

Additionally, we developed a simple, efficient and easy-to-use tool for customers to evaluate their product installations and see if they've experienced any impact because of the issues. The Pulse Security Integrity Checker Tool is available now – we encourage our customers use it and we are working with them to do so.

For customers who believe they are impacted, we are also providing advanced mitigations directly to customers as outlined in our Knowledge Base. Please contact Pulse Secure customer support for help, as needed. Contact +1-844-751-7629 or engage your support representative https://support.pulsesecure.net/support/support-contacts/.

We have been working directly with Mandiant which has released additional findings on the situation. See Mandiant's blog post here.

Customers should be aware that no other Pulse Secure products are impacted by these issues, and they are not connected to any other security or product availability incidents.

A secure computing environment is more important each and every day to how we work and live, as threats evolve and emerge. Ivanti is bullish on Pulse Secure, which was acquired in December 2020, and its other security solutions so that organizations can fully benefit from the changing nature of work. We are making significant investments to enhance our overall cyber security infrastructure, including evolving standards of code development and conducting a full code integrity review.

As an entire company, we are dedicated to working with our customers and the broader security industry to mitigate the threat from these issues as quickly as possible. As our engineering and customer support teams continue to work around the clock to deliver mitigations, we will share updates here.

Thank you,

Phil Richards
CSO