CRITICAL**START** Section 8 Researchers Identify Vulnerability In Paessler's PRTG

Threat intelligence and penetration testing team finds local privilege escalation issue in network monitoring software

Plano, TX – October 3, 2018 – CRITICAL**START**, a leading provider of cybersecurity solutions, today announced its Section 8 threat intelligence and security research team identified a local privilege escalation vulnerability in Paessler's PRTG Network Monitor software. The Section 8 team followed standard vulnerability reporting procedures and alerted Paessler back in July and is presenting the findings today as part of its "Linking to Pwnage! Using Symlinks and Hardlinks to Own All the Things" session at the 11th annual Information Warfare Summit in Oklahoma.

PRTG is an all-in-one unified monitoring solution that makes it easy for system administrators to know what is happening across their entire IT infrastructure, including networks, systems, hardware, applications and devices, at any point in time. Discovered by Quentin Rhoads-Herrera (Paragonsec) during Section 8's ongoing threat intelligence research into symbolic links (symlinks), hardlinks and junctions on Windows, the vulnerability enables a hacker or malicious user to use symlinks to escalate their privileges to gain administrator rights for full access to a specific system or machine.

While there is no vendor advisory, this discovery has been assigned a Common Vulnerabilities and Exposures (CVE) catalog number (CVE-2018-17887) and more information is available in the Section 8 blog post – PRTG Network Monitor Privilege Escalation – with technical details about the vulnerability and an example of how it can be exploited. This PRTG discovery follows Section 8 recently identifying local privilege escalation vulnerabilities in Cisco Umbrella and an unauthenticated command injection vulnerability in VMware's NSX SD-WAN by Velocloud.

"Our research has shown an increase in privilege escalation vulnerabilities due to permission issues and the use of symlinks in a wide variety of software, which in this example is critical given the network monitoring tool's view into a company's networks, applications and systems," said Rhoads-Herrera, offensive security manager for CRITICAL**START**'s Section 8. "While a patch has been released, customers were not proactively notified by the vendor. We are alerting the market so PRTG users can take preventative action to protect their networks if they have not updated their software recently."

In addition to independent threat intelligence and security research, CRITICAL**START**'s Section 8 team delivers high-end offensive security solutions to clients in order to strengthen their information security posture in terms of systems, processes, locations and people. This work includes research, assessments, reports and remediation plans for web application, wireless infrastructure and physical location security, as well as penetration testing and adversarial simulations.

About CRITICAL**START**

CRITICAL**START** is the fastest-growing cybersecurity integrator in North America. Our mission is simple: protect your brand and reduce business risk. We help organizations of all sizes determine their security readiness condition using our proven framework, the Defendable Network. CRITICAL**START** provides managed security services, incident response, professional services, and product fulfillment. Visit www.criticalstart.com for more information.