CRITICAL START'S SECTION 8 RESEARCHERS IDENTIFY VULNERABILITIES IN CISCO UMBRELLA

Threat intelligence and penetration testing team finds local privilege escalation issues in cloud-based secure internet gateway product; Cisco issues security advisory

PLANO, Texas – September 5, 2018 – Critical Start, a leading provider of cybersecurity solutions, today announced its Section 8 threat intelligence and security research team identified local privilege escalation vulnerabilities in Cisco Umbrella. The Section 8 team followed standard vulnerability reporting procedures with Cisco so the vendor could issue a security advisory and patches.

Cisco Umbrella, a secure internet gateway, is a cloud-delivered security platform that protects employees both on and off corporate networks and stops threats over all ports and protocols, including access to malicious domains, URLs, IPs, and files before a connection is ever established or a file downloaded. Discovered during Section 8's ongoing threat intelligence research, the vulnerabilities specifically impacted the Cisco Umbrella Enterprise Roaming Client and Enterprise Roaming Module and would enable a hacker or malicious user to escalate their privileges to gain administrator rights for full access to a specific system or machine.

More details on these vulnerabilities are available:

- **Cisco security advisory:** details on the vulnerability and response for Cisco Umbrella users
- **Section 8 blog:** a post with details about the vulnerability discovered by Quentin Rhoads-Herrera (Paragonsec)
- **Common Vulnerabilities and Exposures (CVE) catalog:** listed as CVE-2018-0437 and CVE-2018-0438

The Cisco Umbrella discovery follows Section 8 recently identifying an unauthenticated command injection vulnerability in VMware's NSX SD-WAN by Velocloud.

"As an increasingly remote and distributed workforce accesses enterprise systems and data through a variety of cloud-based tools, a key part of our research is to ensure the security around those tools is hardened, whether the employee is in the office or a coffee shop across the country," said Quentin Rhoads-Herrera, offensive security manager for Critical Start's Section 8. "Unlike penetration testing 'mills' that simply do quick scans and send check box reports, our team is focused on delivering real value to clients through in-depth analysis, detailed reports and actionable recommendations as well as following responsible disclosure procedures for the security community."

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.

CRITICALSTART