



EmberSec: Senior Security Consultant, Jimmy Bane, Discovers CVE-2019-1378 in Microsoft's Windows 10 Operating System

McLean VA, November 22, 2019 – [EmberSec](#), an advanced cybersecurity services and solutions unit under By Light Professional IT Services, LLC, today announced that Senior Security Consultant, Jimmy Bayne, has discovered and disclosed details of a privilege elevation vulnerability within Microsoft's Windows 10 environment. A fix for [CVE-2019-1378: Exploiting an Access Control Privilege Escalation Vulnerability in Windows 10 Update Assistant \(WUA\)](#) was released as part of Microsoft's "Patch Tuesday" last month.

[Jimmy Bayne](#) was led to this discovery through his dedication to security research. When exploited, this vulnerability gives an attacker privileged access and extensive control of the machine. Read a detailed analysis of the discovery, exploitation, and mitigation walk-through on EmberSec's [blog](#).

"Jimmy's discovery of this vulnerability has provided us with a new insight into what attack vectors adversaries can use to breach our customers and how we can best mitigate them. Our continued mission to discovery and mitigation of these vulnerabilities is what enables EmberSec to better support our customers' risk management practices and guide comprehensive policy reform. Vulnerability research like this is the first step in our triage for building full coverage of our customer's enterprise." -Ken Jenkins, Chief Technology Officer of By Light and Lead of the EmberSec Cybersecurity Team.

Disclosure timeline:

- Mid-September 2019: WUA vulnerability was reported to MSRC.
- Early-October 2019: After continued dialogue between Jimmy and MSRC, MSRC engineers were able to successfully reproduce the vulnerability.
- October 2019 Patch Tuesday: WUA fix was quickly applied since it did not have to go through a check-in process.

New network, application, operating system, and database vulnerabilities emerge on an increasingly frequent basis. Thus, it has become more important than ever to expose security

gaps before malicious actors are able to exploit them. As an integral contributor to EmberSec's specialized risk management services, Jimmy Bayne's expertise in vulnerability discovery and depth of knowledge across Microsoft's technology stack underlines EmberSec's unique positioning to deliver innovative defenses for organizations that leverage one of the largest service providers to businesses worldwide.

EmberSec is a wholly owned subsidiary of By Light Professional IT Services, LLC, based out of McLean, Va. Jimmy has a M.S. degree from Towson University and is CISSP, CISA, OSCP, GPEN, MCSE, PenTest+, and Security+ certified. In his free time, Jimmy helps support the "Living off the Land Binaries & Scripts" (LOLBAS) project.

About By Light Professional IT Services, LLC

By Light Professional IT Services LLC, headquartered in Mclean, VA is an ISO 9001, 20000-1, and 27001 registered and CMMI Level 3 certified systems integrator that provides secure-turn-key systems by incorporating exceptional engineering, project management, telecommunications, and cyber capabilities to safeguard mission success. Founded by industry professionals with extensive knowledge in Defense and government agencies. By Light successfully implements technical solutions that integrate best commercial practices for government, commercial, and international customers. For more information, please visit www.bylight.com.

About EmberSec

EmberSec is comprised of senior security researchers, operators, analysts, hunters and former military intelligence professionals. Our team is powered by a dedication to building relationships that improve the overall security of our customers. We deliver end-to-end cybersecurity services and solutions designed to secure and defend your enterprise.

With deep insights into adversary tactics, techniques and procedures, the EmberSec team begins a unique understanding of security risks in the cyber domain. Skilled in both offensive and defensive cyberspace operations, we offer best-in-breed Technical, Managed and Governance Risk Compliance (GRC) services.

Media Contact

James Ryer
Senior Director, Corporate Communications
By Light, LLC
james.ryer@bylight.com