For immediate release

Once-in-a-decade discovery made by international cyber security company built by former spies

Blackswan = unexpected, tough to detect, easy to exploit, set of seven 0-days found in one week, present in every Windows version since 2007 puts billions of users at risk

(OTTAWA, ON, CANADA - October 14, 2021) Field Effect, a global cyber security company, has released details of their discovery of seven 0-day vulnerabilities in Microsoft Windows software and operating systems. The six privilege escalations and one info leak put billions of Windows users at risk. Dubbed collectively as “Blackswan” by Field Effect due to the unexpected find, the quantity, and the detection challenge, these bugs have amazingly existed in Windows since the 2007 release of Windows Vista.

Such an extensive discovery is extremely rare, and Field Effect estimates that nearly every Windows computer in the world is vulnerable if unpatched, potentially impacting businesses worldwide.

Matt Holland, Founder, CEO, and CTO of Field Effect, says all seven of these vulnerabilities add to a perfect attack scenario and would be easy to utilize as part of a ransomware or nation-state attack chain against businesses of any size and type.

“The Blackswan 0-days are absolute gold for cyber criminals,” said Holland. “If found, they would be very effective from an attacker’s perspective because they are extremely hard to detect, provide access to the deepest layers of the operating system, and can be exploited with 99% reliability. This makes it absolutely critical to keep systems patched and put advanced security measures in place, especially for those businesses that rely on Windows every day.”

The company, an innovator in managed detection and response (MDR), discovered the vulnerabilities in late April 2021, responsibly disclosing its research findings to Microsoft in early May 2021, with proof of concepts and full working exploits.

In its Patch Tuesday updates on July 13, 2021 and September 14, 2021, Microsoft issued patches for the first vulnerability, CVE-2021-34514, and the next five vulnerabilities, including CVE-2021-38628, CVE-2021-38629, and CVE-2021-38638. Patches for the seventh vulnerability CVE-2021-26442 were released on October 12, 2021.

All the Blackswan vulnerabilities were discovered within one week by Field Effect’s security services team, while doing research on the company’s Covalence MDR platform. A vulnerability in the Advanced Local Procedure Call (ALPC) component of the Windows kernel *ntoskrnl.exe* caught their eye — something that was exploitable if triggered in an unexpected way. Upon further investigation, a series of vulnerabilities were found that had similar characteristics.

As Holland explains, the unexpected discovery deserves the moniker “Blackswan” for several reasons. “We weren’t actively threat hunting and certainly didn’t expect to find seven 0-days that could be easily weaponized with only a single week’s effort. What makes these particularly unique is how easily we found them and how long they remained undiscovered in Windows.”

Through its extensive experience with offensive tradecraft techniques, incident response, and intelligence background, Field Effect is continually innovating to expand its Covalence MDR platform to stay ahead of the constantly evolving threat landscape. This commitment to product growth is backed by ongoing, significant investment in research and development, with more than 50% of the company’s revenues invested into technology.

“Our Blackswan discovery reveals just the tip of the iceberg in terms of the amazing calibre of cyber security talent at Field Effect and our commitment to ensuring our customers and partners are protected,” said Holland. “It also underscores the importance for businesses to be diligent with cyber security and invest in a powerful managed security service that effectively detects and blocks threats well before they become serious risks.”

For more detail about Field Effect’s Blackswan vulnerability discovery, read the Field Effect technical blog and view the video discussing the findings.

Additional Resources:

Microsoft Security Report: Patches for CVE-2021-34514 and CVE-2021-38628, CVE-2021-38629, CVE-2021-38638, CVE-2021-26442.

Best practices guide for patch management.

Information about Field Effect’s Covalence MDR platform and customer use cases can be found on our Resources Page.

About Field Effect

Field Effect believes businesses of all sizes deserve powerful cyber security solutions to protect them. The company's threat monitoring and protection, incident response, security training, and consulting services are the result of years of research and development by the brightest talents in the cyber security industry. For more information, visit fieldeffect.com.

#. #. #

Media contact:
Jane Harwood
Director of Marketing
506-378-0177
jharwood@fieldeffect.com