Latest research by Intruder.io reveals the extent to which UK plc is exposed to vulnerabilities in Microsoft products

Submitted by: PR Artistry Limited
Thursday, 26 September 2019

Up to 13,000 organisations, including many FTSE 100 companies, are affected by user enumeration flaws that remain undetected by leading vulnerability scanners

Vulnerability assessment specialists, Intruder.io, today announced its research team has discovered that organisations including almost 40% of the FTSE 100, are affected by little-known user enumeration flaws in a range of popular Microsoft products. The research uncovered that over 13,000 Skype for Business servers on the internet are vulnerable, potentially exposing an organisation's internal Windows network to Denial of Service (DOS) and credential guessing attacks.

Among the list of vulnerable servers are household names and large organisations whose high profile make them likely targets for remote attackers. These include numerous blue-chip companies, some of the 'big four' professional services firms and UK government-owned domains. The flaws have been exposing internal corporate networks to attacks for years and despite being informed of the vulnerability, Microsoft currently has no plans to fix the bugs. This leaves organisations without the usual patch/upgrade option that is often the best solution to fixing security issues.

Chris Wallis, Founder and CEO at Intruder.io, said: "Reconnaissance is an essential stage in every attacker's kill-chain. Companies are facing an increasing challenge to counter the rising numbers of attacks, and anything that makes the attacker's life harder is worth fixing.

"It should never be assumed that software is secure out of the box in its default configuration, and our research illustrates how many companies are exposed to unnecessary risk. Easy-to-use tools are publicly available to exploit vulnerabilities, so attacks against these commonly exposed technologies can be carried out even by unskilled attackers."

User enumeration flaws provide attackers with a method to determine whether a specified username exists. If the attack can be automated, it allows an attacker to whittle down a large list of potential usernames to a smaller list of confirmed usernames. This list of valid usernames for a system is extremely valuable to an attacker because it facilitates a range of other attacks including automated password guessing (brute-force) and DOS attacks. Without the user enumeration flaw to first get a confirmed list of users, these attacks become an order of magnitude more difficult.

Wallis continues: "Organisations should always seek to reduce their perimeter attack surface to a minimum, as a rule of thumb the fewer services are exposed to the Internet, the harder an organisation is to breach. Wherever services must be exposed, regular vulnerability assessments and multi-factor authentication are essential survival tools no organisation should go without."

For advice on how to protect your business read Intruder's research blog: User Enumeration in Microsoft Products: An Incident Waiting to Happen? (https://blog.intruder.io/user-enumeration-in-microsoft-products-an-incident-waiting-to-happen-75c2bba7446c)

NOTES TO EDITORS

About Intruder.io
Intruder.io provides a cloud-based vulnerability scanning service that finds cyber security weaknesses in a company's external infrastructure. With cyber security becoming a top priority for companies of all sizes, Intruder offers an enterprise-grade cyber security solution that works for small to medium sized businesses.
Intruder continually scans an organisation's digital assets, highlighting vulnerabilities and outlining remediation advice to reduce the risk of a breach. It proactively monitors computer systems for emerging threats and provides alerts when an organisation becomes exposed.

Intruder was founded by experts with extensive experience in penetration testing and vulnerability management. The company is headquartered in London, England

For more information please visit Intruder.io (https://intruder.io)
Follow us on Twitter: (https://twitter.com/intruder_io)
Join us on Linked In: (https://www.linkedin.com/company/intruder/)

Press contact:
Andreina West/ Mary Phillips
PR Artistry Limited
T: +44 (0)1491 845553
E: andreina@pra-ltd.co.uk