CHUBB®

Stay Ahead: Be Informed, Act Swiftly Against Vulnerabilities

In today's constantly evolving digital landscape, businesses of all sizes find themselves under the constant threat of cybersecurity breaches. According to Cybersecurity Infrastructure Security Agency (CISA), 50% of known exploited vulnerabilities (KEVs) are exploited within two days of being identified and 75% are exploited in less than a month. It is imperative to have a vulnerability management program in place to act fast and remediate before malicious activity enters and spreads throughout an organization's network.

Chubb Dynamic Vulnerability Detection

With our Vulnerability Management Outreach, our Cyber Intelligence Team routinely monitors, scans, and identifies vulnerabilities and new critical threats to help safeguard our policyholders. Policyholders who register to receive alerts are informed by:

Outreach Programme - a proactive notification to cyber policyholders if identified known critical vulnerabilities are detected to be in their environment and have a high probability of exploitation.

- An initial communication via email, which details the exposure and actions required to remediate.
- Follow-ups, which are then conducted via email and phone calls.

Breaking Alerts - are sent to cyber policyholders when new vulnerabilities with a high probability of exploitation are discovered and may impact their environment.

- A communication via email, with information on the new threat is generally sent within 24 hours of discovery.

Additional Cyber Vulnerability Management Solutions

In addition to our Vulnerability Management Outreach, all Chubb Cyber policyholders are eligible to register for the following complimentary cyber services:

- **External Vulnerability Monitoring** - In partnership with BitSight, policyholders can monitor cyber risk as a daily measurement of their security performance via a platform that uses key metrics to highlight both strengths and potential weaknesses, providing visibility into the security of their organization.

To register for Chubb's Vulnerability Management Outreach programme and to get more information on Chubb Cyber Services, please visit www.chubb.com/nordic-en/cyber-service-form/nordics-cyber-services

Chubb Vulnerability Outreach Program

Red Flag Alerts FAQs

General FAQs

What is the purpose of Chubb Vulnerability Outreach program?

- The purpose is to notify organizations of their exposure to high-risk vulnerabilities and other severe misconfigurations (open ports, malware infections, etc.). Chubb has adopted this approach in order to alert and assist policyholders in identifying and remediating internet-facing issues our threat intelligence team has classified as high-risk exposures. As such, each of the vulnerabilities we identify can and will be identified by threat actors. Additionally, the list of vulnerabilities Chubb scans for are considered highly exploitable in the wild.

Why is Chubb alerting me to vulnerabilities in my environment?

- This is an important part of the symbiotic relationship of Chubb and our policyholders. We have been providing risk engineering services to our policyholders throughout the world for over one hundred years, which makes our policyholders better managers of risk, and Chubb better as underwriters. Cyber is no different. As we identify vulnerabilities that are causing losses or are on high-risk cyber intelligence lists that we can see in our policyholders' environments, we work to reduce exposure to those vulnerabilities as a priority.

Do these alerts have any impact on coverage?

- No. However, an unwillingness to take action to remediate these prioritized vulnerabilities may have an impact on the underwriting of your policy in the future. For example, if we continuously see these vulnerabilities and no response or action from a policyholder, we may consider not renewing coverage.

Is this a Penetration Test?

- This is not a penetration test. There is no active scanning or attempts at infiltrating your environment. This process utilizes external passive scanning platforms which utilize a combination of open-source intelligence (OSINT) and passive scanning. Passive scanning is non-intrusive and a safe methodology to identify internet-facing assets and any potential vulnerabilities or misconfigurations associated with them.

Red Flag Alerts FAQs

Why am I getting this?

- You are receiving this alert as you have registered for the Chubb Vulnerability Outreach Program, available for our Policyholders as a complementary service with their Cyber policy. It relates either to a known exploited vulnerability (KEV) or any other severe cybersecurity finding that was detected via non-intrusive external scanning tools such as BitSight and Security Scorecard. The alert includes information that the insured's IT team can use to identify and remediate the exposed asset.

What if I don't understand these alerts?

- The Cyber Intelligence Team at Chubb is happy to discuss this process and the alert details with anyone in your organization. You may also forward it on to your internal information security professional or a third-party MSP who oversees your environment for any clarifications and/or insights.

I don't know what this is or what to do about it, can you help?

- Yes, you can request a General Support call with Chubb's Cyber Risk Advisory Team by reaching out to Cyber@chubb.com
- Please be sure to add a comment indicating you received a vulnerability alert and wish to discuss.

This isn't my IP address. Is any action needed?

- Please forward the alert to Cyber@Chubb.com noting the specific misattributed IP addresses and we will update our records indicating they relate to a non-insured asset. If interested, the Chubb Cyber Risk Advisory team can provide instructions for your IT team to submit an inquiry for these findings via Bitsight or Security Scorecard to prevent future automated alerts pertaining to these misattributed IPs.

This is not my domain.

- Please reach out to Cyber@Chubb.com with confirmation of the correct domain and Chubb will ensure your policy is updated to reflect it. We will then update our records to show that the vulnerability relates to a non-insured asset and close the related case.

All Cyber services are subject to change. Any changes to the service offering will be reflected on the local Cyber services webform. Policyholders are responsible for reviewing specific terms and conditions of each cyber service provider to ensure eligibility and to stay updated on any changes that may occur.

DISCOUNTED CYBER SERVICES OFFERED BY THIRD PARTY VENDORS:

External Vulnerability Monitoring, Secure Password Manager
The cyber services set forth above are offered by third party vendors at no additional cost to Chubb policyholders for the stated initial period, provided the policyholder is a new subscriber/customer to the cyber services on offer by the chosen third-party vendor and the policyholder otherwise meets the stated eligibility requirements. After expiration of the stated initial period, policyholders may have the option to continue their cyber services at a discounted rate upon renewal. Please note that the specific discount may vary between products and services. Discounts on products and services offered by cyber services vendors are available only to Chubb policyholders with current in-force policies and are subject to applicable insurance laws. The products and services provided by third party vendors will be governed by contract terms the policyholder enters into with the third-party vendor. Chubb will not be involved in the policyholder's decision to purchase services and has no responsibility for products or services that are provided by any third-party vendor.

Chubb European Group SE, Swedish Branch, is registered in the company register with the corporate registration number 516403-5601 and the visiting adress Birger Jarlsgatan 43, 111 45 Stockholm. Chubb European Group SE is an undertaking governed by the provisions of the French insurance code with registration number 450 327 374 RCS Nanterre and the following registered office: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Chubb European Group SE has fully paid share capital of €896,176,662 and is supervised by the Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09. The branch's operations are also subject to supervision by the Swedish FSA (Finansinspektionen).

We use personal information which you supply to us [or, where applicable, to your insurance broker] for underwriting, policy administration, claims management, and other insurance purposes, as further described in our Master Privacy Policy, available here: http://www.chubb.com/nordic-en/footer/privacy-policy.html.