Urgent Alert for e-Commerce Vendors

The United States Secret Service has detected a significant upsurge in e-Skimming attacks due to an increase in online shopping.

E-Skimming

E-Skimming targets businesses accepting online payments. Often called "Magecart" attacks by researchers, cybercriminals leverage vulnerabilities, known and unknown, to modify stores' source code to steal payment card data in real time.

Magento Platform

The Secret Service specifically noted a campaign targeting online stores running legacy versions of the open source e-commerce platform Magento. All versions of Magento 1 are considered end-of-life (EOL) as of June 30, 2020, meaning no further vendor security patches are forthcoming. Magento still provides support for its Open Source 2 product. An estimated 75,000 live sites are currently operating on Magento 1 platforms, highlighting the target-rich environment that exists for cybercriminals looking to take advantage of the ease and high profitability of e-skimming.

Recommended Risk Mitigations

- Keep all systems patched and up-to-date, to include operating systems, software, and any third-party code running as part of your website.
- Do not use default login credentials on any system.
- Keep web application firewalls strong and monitor administrative activity.
- Eliminate/disable functions within your online store that are not necessary.

  Monitor requests performed against your store's environment to identify possible malicious activity (loader and exfiltration domains).

Contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF).

https://www.secretservice.gov/contact/field-offices/