ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

CTI-ADV-2025-02

TLP:CLEAR

Critical Vulnerability (CVE-2018-19410) Exposes 600 PRTG Instances in Bangladesh

[This page is intentionally left blank]

TLP: CLEAR
Distribution: Public
Date: 17 February 2025

Executive Summary

As part of BGD e-GOV CIRT continuous efforts to monitor emerging threats and vulnerabilities that could compromise national security, our Cyber Threat Intelligence Unit has identified **600** vulnerable PRTG instances in Bangladesh affected by **CVE-2018-19410**—a critical-severity vulnerability. This **Local File Inclusion (LFI) and Authentication Bypass** flaw is actively exploited by cybercriminals and is listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog. This vulnerability, affecting PRTG Network Monitor versions **before 18.2.40.1683**, allows remote unauthenticated attackers to create users with read-write (admin) privileges, granting them full control over the instance. Exploiting this flaw could lead to unauthorized access, data exfiltration and system manipulation, posing a significant risk to the system's confidentiality and integrity. Immediate remediation is critical to prevent further exploitation.

Vulnerability Details

- **CVE ID:** CVE-2018-19410
- **CVE Type:** Authentication Bypass, Improper Authorization, Local File Inclusion (LFI)
- **Severity:** 9.8 Critical
- **Attack Vector:** Remote
- **Exploitability:** Unauthenticated remote attackers can create users with admin privileges

Affected Software

- **Software:** PRTG Network Monitor
- **Affected Versions:** earlier than 18.2.40.1683

Attack Method

- The flaw exists in **/public/login.htm**, where an attacker can override attributes of the 'include' directive.
- Attackers can include **/api/addusers** in the request, allowing unauthorized user creation with read-write (admin) privileges.
- This leads to authentication bypass, improper authorization, and file inclusion attacks.

Potential Impact

- **Complete system compromise** by unauthorized attackers.
- **Privileged access** for malicious users.
- **Execution of arbitrary code** through unauthorized file inclusion.
- **Data theft and operational disruption** in affected networks.

Bangladesh among the Most Affected Countries

A significant number of **600** vulnerable instances have been detected in Bangladesh, running outdated PRTG versions.

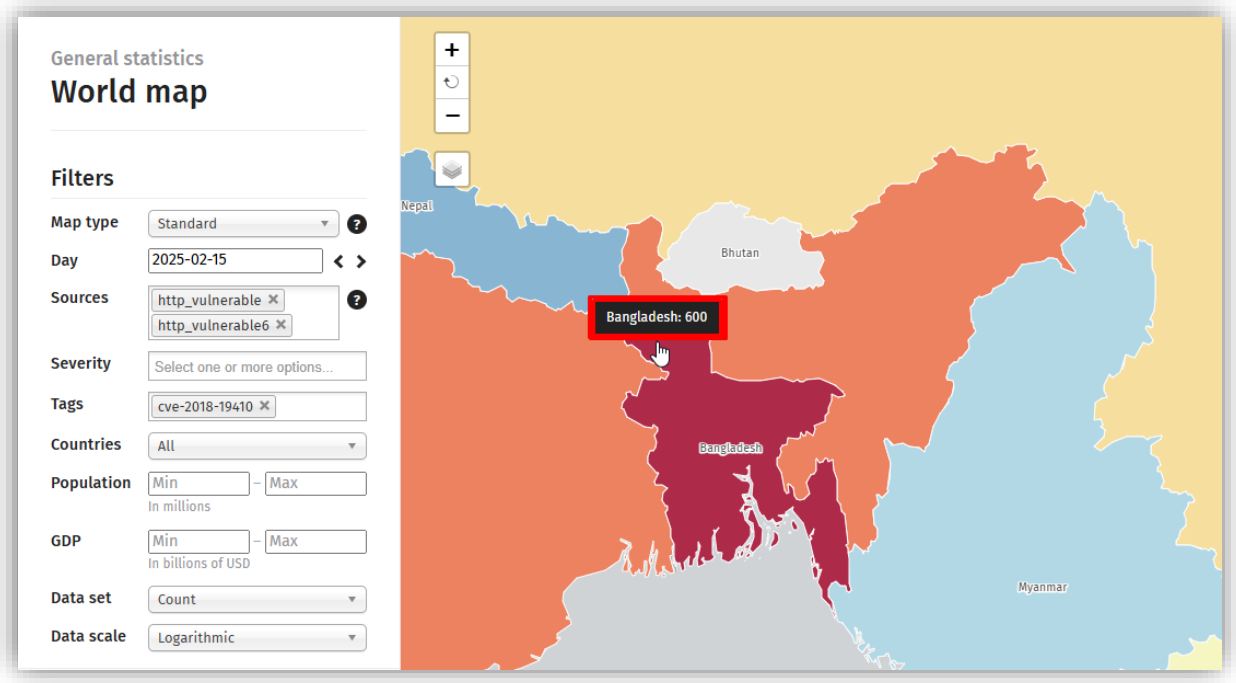

Figure: 600 vulnerable PRTG instances detected in Bangladesh (Source: Shadowserver)

- Identified Vulnerable Versions in Bangladesh:

17.3.32.2478	*17.3.33.2753*	*13.1.2.1462*
7.2.5.5114	*17.3.33.2830*	

Indicators of Compromise (IoCs)

- **Suspicious Logs**:
- Unusual requests to /public/login.htm
- Unauthorized execution of /api/addusers
- Unexpected admin account creation in PRTG logs
- **File System Changes:**
- Unauthorized user account modifications/creation
- Unexpected configuration changes in the PRTG system
- **Network Anomalies:**
- High-volume HTTP requests targeting PRTG login pages
- Unauthorized administrative actions from unknown IP addresses

Mitigations & Recommended Actions

To mitigate the risks associated with CVE-2018-19410, organizations using PRTG Network Monitor versions before 18.2.40.1683 should implement the following security measures:

Upgrade PRTG Immediately

- Update to the latest Paessler PRTG Network Monitor version

Check for Indicators of Compromise (IoCs)

- Review PRTG logs for unauthorized account creation.
- Scan your environment for suspicious login attempts and file modifications.

Restrict Access & Hardening

- Limit access to PRTG web interface to trusted internal networks only.
- Implement multi-factor authentication (MFA) for administrator accounts.

Monitor for Threat Activity

- Deploy Intrusion Detection Systems (IDS) to detect suspicious activity.
- Continuously monitor SIEM alerts for unusual user behavior.

Network Segmentation

- Isolate PRTG servers from internet exposure where possible.