SEQURETEK

VULNERABILITIES IN TREND MICRO IWSVA

OVERVIEW

The Trend Micro InterScan Web Security Virtual Appliance (IWSVA) is affected by multiple critical security issues. Unauthenticated attackers are able to gain root access to the appliance via chained attack vectors, such as CSRF protection bypass, authorization & authentication bypass, command execution and unauthenticated command injection vulnerabilities.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
21st Dec 2020	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- Trend Micro has made a Critical Patch available for Trend Micro **InterScan Web Security Virtual Appliance (IWSVA) 6.5 SP2**.
- Trend Micro **IWSVA is a web gateway that helps enterprises protect their systems against online threats,** while also providing real-time visibility and control of employee internet usage.
- Released Critical Patch addresses multiple vulnerabilities related to CRSF protection bypass, cross-site scripting (XSS), authorization/authentication bypass, command execution and unauthenticated command injections.

By exploiting these vulnerabilities,

1. An attacker **can gain root access to a targeted appliance remotely** from the internet by chaining the CSRF and command execution vulnerabilities.
2. An attacker with **access to the HTTP proxy port could exploit the authentication/authorization bypass vulnerabilities and the command execution flaw** to take over the appliance as root, without user or admin interaction.
3. An attacker with network access to the admin interface could exploit the command injection vulnerability which affects the login process under certain configurations to execute arbitrary OS commands on the appliance as a user named "iscan" and possibly elevate privileges.

VULNERABILITY DETAILS

- **CVE-2020-8461: CSRF Protection Bypass (CVSSv3: 7.1)**
  This vulnerability could allow an attacker to get a victim's browser to send a specifically encoded request without requiring a valid CSRF token.
- **CVE-2020-8462, CVE-2020-27010: Cross-Site Scripting (CVSSv3: 3.3)**
  This vulnerabilities could allow an attacker to tamper with the web interface of the product.
- **CVE-2020-8463: Authorization Bypass(CVSSv3: 8.2)**
  This vulnerability could allow an attacker to bypass a global authorization check for anonymous users by manipulating request paths.
- **CVE-2020-8464: Authentication Bypass/SSRF (CVSSv3: 8.2)**
  This vulnerability could allow an attacker to send requests that appear to come from the localhost which could expose the product's admin interface to users who would not normally have access.

- **CVE-2020-8465: Command Execution(CVSSv3: 8.2)**

  This vulnerability could allow an attacker to manipulate system updates using a combination of CSRF bypass (CVE-2020-8461) and authentication bypass (CVE-2020-8464) to execute code as user root.

- **CVE-2020-8466: Unauthenticated Command Injection(CVSSv3: 8.2)**

  This vulnerability, with the improved password hashing method enabled, could allow an unauthenticated attacker to execute certain commands by providing a manipulated password.

AFFECTED VERSIONS

PRODUCT	AFFECTED VERSION(S)	PLATFORM	LANGUAGE(S)
IWSVA (InterScan Web Security Virtual Appliance)	6.5 SP2	Virtual Appliance	English

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- Update to Trend Micro IWSVA version 6.5 SP2 CP b1919.
- Enable Management Access Control in IWSVA to set ACLs that restrict access to the management console to a specific IP or IP range that are trusted in your organization.
- Limit IP access to the IWSVA management console.