





SECURITY BULLETIN: Multiple Vulnerabilities in Trend Micro InterScan Messaging Virtual Appliance (IMSVA) 9.1

Product/Version includes: InterScan Messaging Security Virtual Appliance 9.1, [View More](#)

-  **Update Date:** 2021/04/21
-  **Article Number:** 000279833
-  **Category:** Upgrade, Update
-  **Rating:** 0

Summary

Release Date: November 4, 2020
CVE Identifier(s): CVE-2020-27016, 27017, 27018, 27019, 27693, 27694
Platform(s): Virtual Appliance
CVSS 3.0 Score(s): 2.8 - 7.6
Severity Rating(s): Low - High

Trend Micro has released a new Critical Patch (CP) for Trend Micro InterScan Messaging Virtual Appliance (IMSVA) 9.1. This CP resolves multiple vulnerabilities related to cross-site request forgery (CSRF), XML external entity processing (XXE), server side request forgery (SSRF), information disclosure, insufficient password storage and outdated software components.

Affected Version(s)

Product	Affected Version(s)	Platform	Language(s)
IMSVA	< 9.1.0 CP B2025	Windows	English

Solution

Trend Micro has released the following solutions to address the issue:

Product	Updated version	Notes	Platform	Availability
IMSVA	Version 9.1 CP B2025 (https://files.trendmicro.com/products/imsva/9.1/imsva_91_en_critical_patch_b2025.tar.gz)	Readme (https://files.trendmicro.com/documentation/readme/imsva_91_en_criticalpatch_b2025_EN_Readme.txt)	Virtual Appliance	Now Available

This is the minimum version(s) of the patch and/or build required to address the issue. Trend Micro highly encourages customers to obtain the latest version of the product if there is a newer one available than the one listed in this bulletin.

Customers are encouraged to visit Trend Micro's Download Center (<http://downloadcenter.trendmicro.com/>) to obtain prerequisite software (such as Service Packs) before applying any of the solutions above.

Vulnerability Details

This update resolves multiple vulnerabilities in Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA):

1. **CVE-2020-27016** (7.5 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:H) - Cross-Site Request Forgery (CSRF)
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to a cross-site request forgery (CSRF) vulnerability which could allow an attacker to modify policy rules by tricking an authenticated administrator into accessing an attacker-controlled web page.

Please note that an attacker must already have obtained product administrator/root privileges to exploit this vulnerability.

2. **CVE-2020-27017** (7.6 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L) - XML External Entity Processing (XXE)
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to an XML External Entity Processing (XXE) vulnerability which could allow an authenticated administrator to read arbitrary local files.

Please note that an attacker must already have obtained product administrator/root privileges to exploit this vulnerability.

3. **CVE-2020-27018** (2.8 CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:U/RL:X/RC:X) - Server Side Request Forgery (SSRF) and Local File Disclosure
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to a server side request forgery vulnerability which could allow an authenticated attacker to abuse the product's web server and grant access to web resources or parts of local files.

Please note that an attacker must already have obtained authenticated privileges on the product to exploit this vulnerability.

4. **CVE-2020-27019** (4.8 CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L/E:U/RL:X/RC:X) - Information Disclosure
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA) 9.1 is vulnerable to an information disclosure vulnerability which could allow an attacker to access a specific database and key.

5. **CVE-2020-27693** (3.1 CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:L/E:U/RL:X/RC:X) - Insufficient Password Storage
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVa) 9.1 stores administrative passwords using a hash that is considered outdated.

6. **CVE-2020-27694** (4.6 CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:U/RL:X/RC:X) - Outdated Library
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVa) 9.1 has updated a specific critical library that may be vulnerable to an attack.

Due to the seriousness of these and any vulnerabilities, customers are highly encouraged to update to the latest build as soon as possible.

Mitigating Factors

Exploiting these type of vulnerabilities generally require that an attacker has access (physical or remote) to a vulnerable machine. In addition to timely application of patches and updated solutions, customers are also advised to review remote access to critical systems and ensure policies and perimeter security is up-to-date.

However, even though an exploit may require several specific conditions to be met, Trend Micro strongly encourages customers to update to the latest builds as soon as possible.

Acknowledgement

Trend Micro would like to thank the following individuals for responsibly disclosing these issues and working with Trend Micro to help protect our customers:

- W. Ettlinger and T. Serafin of SEC Consult Vulnerability Lab (<https://www.sec-consult.com>)

External Reference(s)

- SEC Consult Advisory (<https://sec-consult.com/en/blog/advisories/vulnerabilities-in-trend-micro-interscan-messaging-security-virtual-appliance-imsva/>)