Cybersecurity Vulnerability Statements

Assessment and Communication Process

The Allied Telesis Security Monitoring team monitors incidents and vulnerabilities that may affect Allied Telesis products. Our Net.Cover maintenance plans allow you to obtain the latest software updates to ensure your network is free from known vulnerabilities.

Latest Vulnerability Statement

Apache Log4j vulnerability

(published 14 Dec 2021; last updated 6 March 2022)

A high severity vulnerability, CVE-2021-44228, has been reported in Apache Log4j, a popular Java logging package. The Allied Telesis Cybersecurity Team has reviewed the vulnerability and assessed its impact on Allied Telesis network products.

No current Allied Telesis products are considered vulnerable. In the unlikely event that you are using a version of Vista Manager EX earlier than 3.0.3, we recommend upgrading as an additional safeguard.

Details are as follows:

- AlliedWare Plus switches and routers/firewalls: Not Affected
- Device GUI for AlliedWare Plus products: Not Affected
- The Vista Manager Network Appliance (VST-APL) and Vista Manager Virtual (VST-VRT): Not Affected
- The 10G Virtual UTM Firewall: Not Affected
- AMF Security: Not Affected
- Non-AlliedWare Plus switches and routers/firewalls: Not Affected
- Access Points: Not Affected
- Media converters: Not Affected
- AlliedView NMS Standard Edition: Not Affected
- Vista Manager EX: Not Affected (except for some no-longer-used early versions—see below for details).

Vista Manager EX

Log4j is used by one of Vista Manager EX's components. The impact on Vista Manager EX and its AWC and SNMP plugins is as follows:

- Vista Manager EX versions 3.0.3 and newer: Not Affected
- Vista Manager EX versions 2.5 – 3.0.2, Windows platform: Vulnerable but unlikely to be exploitable (see below for details)
- Vista Manager EX versions 2.5 – 3.0.2, all other platforms: Not Affected
- Vista Manager EX all other versions: Not Affected
- Vista Manager EX AWC Plug-in all versions: Not Affected
- Vista Manager EX SNMP Plug-in all versions: Not Affected

Note that some vulnerability scanning tools may indicate that Vista Manager EX uses vulnerable versions of the library. However, the vulnerability can only be exploited if the library is used with certain older versions of Java, which Vista Manager EX does not use in versions 3.0.3 and newer. Therefore, these versions of Vista Manager EX are not vulnerable. If you wish to prevent your vulnerability scanning tool from incorrectly indicating that Vista Manager EX uses vulnerable versions of the library, upgrade to Vista Manager EX version 3.8.1 (or later), available from our Software Download center.

Vista Manager EX versions 2.5 – 3.0.2, Windows platform

These no-longer-used early versions of Vista Manager EX use a version of Logstash that Elasticsearch B.V. has stated is vulnerable to this attack. However, since its use in Vista Manager EX is limited, the Allied Telesis Cybersecurity Team has not been able to exploit the vulnerability.

Therefore, it is unlikely that an attacker would be able to use this vulnerability to compromise these versions of Vista Manager EX.

Recommended Action: In the unlikely event that you are using one of these versions, upgrade to an unaffected version of Vista Manager EX, preferably the latest version.