Q4 - 2020 November 18, 2020

IMPACT LEVEL: Immediate

Cisco - Releases Security Updates for ‘Security Manager’

- Cisco has released security updates to address vulnerabilities in Cisco Security Manager
- A remote attacker could exploit these vulnerabilities to obtain sensitive information
- Cisco has flagged that the three security vulnerabilities are fixed in version 4.22 of Cisco Security Manager, which was released last week
- The issue, with a severity rating of 9.1 out of 10, affects Cisco Security Manager releases 4.21 and earlier
- Cisco Security Manager helps admins manage security policies on Cisco security devices and provision Cisco's firewall, virtual private network (VPN), Adaptive Security Appliance (ASA) devices, Firepower devices, and many other switches and routers
- The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and administrators to review the Cisco security advisory pages (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR, https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-rce-8gjUz9fW) and apply the necessary update

Source(s)

https://us-cert.cisa.gov/ncas/current-activity/2020/11/17/cisco-releases-security-updates-security-manager
https://www.zdnet.com/article/cisco-reveals-this-critical-bug-in-cisco-security-manager-after-exploits-are-posted-patch-now/

Targets Affected:

Cisco

Category(s):

Cyber Security Risk

Event:

Coronavirus (COVID-19) Incident(s)

Guidance

Actions to consider:

- It is important for SW Subscribers to determine whether all of Cisco's recommended mitigation steps and mandated upgrades are assessed and implemented
- It is recommended for SW Subscribers to regularly audit applications which are installed in the devices and review all internal, sourcing and service partners' networks, who may also be impacted by Cisco's vulnerability and ensure that they have completed the required patches and updates
- Determine if the third party regularly tests its networks for vulnerabilities and potential risks and errors and has a well-documented response plan in place, which helps it detect glitches as well as notify concerned parties in a timely and effective manner
- SW Subscribers should request third party to share results of vulnerability tests with them without fail
- It is advised to follow cyber security alerts monitored by Supply Wisdom, regularly check advisories issued/emailed directly by Cisco, update systems as soon as possible and follow any other instructions provided by the third party
- In the era of widespread prevalence of cyber-security threats, it is crucial for SW Subscribers to have an independent cyber assessment of the concerned third parties done on a real-time basis, such as the recently expanded cyber susceptibility review service from Supply Wisdom, which has been designed to ensure that SW

Subscribers have necessary information about the cyber health of their third-parties

Impact level Definitions

Impact Level	Definitions
Immediate	**Certain** - Supply Wisdom recommends considering prompt action. Examples of Immediate level alert events may include bankruptcy filings, data breaches, unexpected curfews, strikes, power black-outs, major geo-political events etc.
High	**Highly likely to occur in the near term (within 3 months)** - Supply Wisdom recommends being in a state of readiness to take quick action. Examples of High level alert events may include withdrawal of rating by ratings agencies, hostile takeover, multiple cyber-attacks, new business policies causing significant hardship etc.
Medium	**Likely to occur in the mid-term (within 3 to 6 months)** - Supply Wisdom recommends reviewing current mitigation steps and being ready to take proactive actions if and when situation deteriorates further. Examples of Medium level alert events may include unplanned C-level exits, suppliers caught in bribery cases, economy slipping into recession.
Low	**Possible in the long-term (after 6 months)** - Supply Wisdom recommends taking proactive action if situation does not resolve. Examples of Low level alert events may include lawsuits filed against suppliers, client losses, air pollution alerts issued by country's local authorities, unexpected holidays announced for the location etc.
Informational	The event is pertinent information but does not have a risk element associated with it. Examples of Info level alert events may include launch of new solutions, partnerships signed, industry outlook, positive changes in government policies, announcements regarding launch of software parks/ free trade zones/special economic zones etc.