ADV2025_300 Cisco Security Advisory (September 3rd, 2025)

Cisco has published a security advisory highlighting vulnerabilities in the following products on August 27th, 2025. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Cisco UCS 6300 Series Fabric Interconnects
- Cisco Catalyst 8300 Series Edge uCPE
- Cisco UCS Manager Software
- Cisco UCS B-Series Blade Servers
- Cisco UCS C-Series M6, M7, and M8 Rack Servers
- Cisco UCS E-Series Servers M6
- Cisco UCS X-Series Modular System
- Cisco MDS 9000 Series Multilayer Switches
- Cisco Nexus 1000 Virtual Edge for VMware vSphere
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 5500 Platform Switches
- Cisco Nexus 5600 Platform Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series Fabric Switches in ACI mode
- Cisco Nexus 9000 Series Switches in standalone NX-OS mode
- Cisco UCS 6400 Series Fabric Interconnects
- Cisco UCS 6500 Series Fabric Interconnects
- Cisco UCS X-Series Direct Fabric Interconnect 9108 100G
- Cisco Nexus Dashboard 3.2 and earlier
- Cisco Nexus Dashboard 4.1
- Cisco Nexus Dashboard Fabric Controller (NDFC)

For more information on these updates, you can follow this URL:

Cisco Security Advisories

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Cisco Security Advisories. (August 27th, 2025). Retrieved from Cisco. https://sec.cloudapps.cisco.com/security/center/publicationListing.x

- Cisco Security Advisory. (August 27th, 2025). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av25-547