U.S. DEPARTMENT OF STATE OFFICE OF INSPECTOR GENERAL
INVESTIGATIONS

FRAUD ALERT 2501
Grey Market Cisco Devices

The Office of Inspector General (OIG) determined that various Cisco Systems, Inc. (Cisco) branded devices purchased by the U.S. Department of State (Department) were non-genuine products that posed significant threats to Department networks. OIG and Diplomatic Technology (DT) discovered these non-genuine devices were purchased from unauthorized "grey market" vendors outside of the Department's standard Supply Chain Management process.

Unauthorized vendors often engage in the sale of counterfeit products and may intentionally conceal the true nature of their business from potential buyers. These non-genuine grey market devices fail to meet critical standards related to quality, performance, and security. They have not undergone rigorous testing and lack the reliable components found in authentic products, which may lead to vulnerabilities, compatibility issues, and potential safety hazards. Furthermore, these devices do not provide access to legitimate firmware updates, warranties, or technical support, and they often fail to comply with necessary regulatory requirements.

Here are some common tactics used by unauthorized Cisco vendors to mislead customers:

1. **Counterfeit Products:** Unauthorized vendors produce devices that look like genuine Cisco products, but lack the quality features, security, and support associated with authentic Cisco hardware.
2. **Tampered Serial Numbers**: Some unauthorized vendors alter or forge serial numbers to make counterfeit devices appear legitimate.
3. **Inaccurate Specifications:** Fraudulent devices are marketed with misleading specifications. They claim to have the capabilities of specific Cisco devices but do not perform as advertised or lack essential features.
4. **No Software or Firmware Support:** Unauthorized devices come without legitimate software licenses or updates, leaving customers vulnerable to security and performance issues.
5. **Fake Warranty and Support:** Unethical vendors offer warranties and support that are not honored. When problems arise, customers cannot obtain assistance or replacement parts.
6. **Misleading Branding:** Some vendors sell counterfeit devices under the Cisco brand or confuse customers with similar branding to create an illusion of legitimacy.
7. **Drop-Shipping:** In some cases, an unauthorized vendor does not have the devices at all. Instead, they ship counterfeit devices from other sources, leading to vulnerabilities in product quality and authenticity.

To avoid becoming victims of counterfeit Cisco devices, organizations adopted several key strategies:

1. **Buying from Authorized Resellers:** Purchase only from DT/SCM's enterprise agreement or verified Cisco partners to ensure authenticity.
2. **Checking Serial Numbers:** Verify serial numbers through Cisco's support portal to confirm legitimacy.
3. **Researching Specifications:** Familiarize yourselves with genuine product specifications to detect discrepancies.
4. **Inspecting Packaging:** Look for high-quality packaging and documentation typical of authentic products.
5. **Verifying Software Licenses:** Ensure that any included software has valid licenses to mitigate risks.
6. **Utilizing Official Support:** Contact Cisco for official support whenever issues arise with products.
7. **Being Cautious with Payment Methods:** Avoid vendors with unusually low prices or atypical payment requests.
8. **Reporting Suspicions:** Report suspicious vendors to Cisco, OIG, and relevant Bureaus.
9. **Educating Teams:** Provide training on how to identify authorized vendors and authentic products.
10. **Conducting Regular Audits:** Perform regular checks to verify the authenticity of network equipment.
11. **Assessing How Shipments Arrive:** Do not install devices that did not arrive at your post through a secure procurement and shipping process.

By implementing these measures, organizations significantly reduced the threat of acquiring counterfeit devices.

If you have information about fraud, waste, abuse or mismanagement, as well as other crimes or violations of Federal laws, rules, and regulations relating to Department programs and operations, please report it to the OIG Hotline. You can submit your complaint at stateoig.gov/hotline. The Hotline may be used for unclassified information only. To submit classified information, contact the Hotline at (800) 409-9926 or (202) 647-3320 for further instruction.

HELP FIGHT

FRAUD, WASTE, AND ABUSE

1-800-409-9926

Stateoig.gov/HOTLINE