Advisory Alert

Alert Number: AAA20240926 **Date:** September 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WatchGuard	**Critical**	Multiple Incorrect Authorization Vulnerabilities
NetApp	**High**	Security Update
WatchGuard	**High**	Improper Handling of Exceptional Conditions Vulnerability
Cisco	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Incorrect Authorization Vulnerabilities (CVE-2024-6592, CVE-2024-6593)
Description	WatchGuard has released security updates addressing Multiple Incorrect Authorization Vulnerabilities that exist in their products. **CVE-2024-6592** - An incorrect authorization vulnerability in the protocol communication between the WatchGuard Authentication Gateway on Windows and the WatchGuard Single Sign-On Client on Windows and MacOS allows an attacker with network access to forge communications to affected components. **CVE-2024-6593** - An incorrect authorization vulnerability in WatchGuard Authentication Gateway on Windows allows an attacker with network access to execute restricted management commands. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Authentication Gateway: through 12.10.2 Windows Single Sign-On Client: through 12.7 MacOS Single Sign-On Client: through 12.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00014 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00015

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-45288)
Description	NetApp has released security updates addressing a vulnerability that exists in FreeBSD third party product that affects ONTAP 9. Successful exploitation of this vulnerability could lead to disclosure of information, addition or modification data, or Denial of Service. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 versions prior to 9.14.1P8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240920-0008/

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Improper Handling of Exceptional Conditions Vulnerability (CVE-2024-6594)
Description	WatchGuard has released security updates addressing an Improper Handling of Exceptional Conditions Vulnerability that exists in their products. **CVE-2024-6594** - An improper handling of exceptional conditions vulnerability in the WatchGuard Single Sign-On Client on Windows causes the client to crash while handling malformed commands. An attacker that has gained network access could create a denial-of-service (DoS) condition for the Single Sign-On client, preventing the computer from completing the SSO process by repeatedly issuing malformed commands. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Windows Single Sign-On Client: through 12.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00016

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20437, CVE-2024-20455, CVE-2024-20433, CVE-2024-20464, CVE-2024-20480, CVE-2024-20436, CVE-2024-20350, CVE-2024-20467, CVE-2024-20381, CVE-2024-20434, CVE-2024-20508, CVE-2024-20475, CVE-2024-20496, CVE-2024-20465, CVE-2024-20414, CVE-2024-20510)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Command Execution, Denial of Service, Privilege Escalation, Cross-Site Scripting, Cross-Site Request Forgery. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-csrf-ycUYxkKO • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-utd-dos-hDATqxs • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rsvp-dos-OypvgVZf • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pim-APbVfySJ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-MBcbG9k • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-httpsrvr-dos-yOZThut • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ssh-e4uOdASj • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpp-vfr-dos-nhHKGgO • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-auth-bypass-QnTEesp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vlan-dos-27Pur5RT • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-utd-snort3-dos-bypas-b4OUEwxD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-xss-zQ4KPvYd • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-vedos-KqFfhps3 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-repacl-9eXgnBpD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-HfwnRgk • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-cwa-acl-nPSbHSnA

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31355, CVE-2024-21978, CVE-2024-21980, CVE-2023-48795, CVE-2024-20399, CVE-2023-31315, CVE-2024-21801, CVE-2024-22374, CVE-2024-21810, CVE-2024-23497, CVE-2024-23981, CVE-2024-24986, CVE-2024-21807, CVE-2024-21769, CVE-2024-24983, CVE-2024-23499, CVE-2024-21806, CVE-2024-22376, CVE-2024-24853, CVE-2024-24980, CVE-2023-42772, CVE-2023-22351, CVE-2023-25546, CVE-2023-41833, CVE-2023-43753, CVE-2024-21781, CVE-2024-21829, CVE-2024-21871, CVE-2024-24968, CVE-2024-23984, CVE-2024-6387, CVE-2024-25561, CVE-2024-28970, CVE-2023-49141, CVE-2023-42667, CVE-2022-1012, CVE-2022-32296, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000228917/dsa-2024-233-security-update-for-dell-connectrix-cisco-mds-9000-series-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227518/dsa-2024-306-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227665/dsa-2024-344-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227763/dsa-2024-359-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-and-tdx-software-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227762/dsa-2024-308-security-update-for-dell-poweredge-server-for-intel-august-2024-security-advisories-2024-3-ipu • https://www.dell.com/support/kbdoc/en-us/000227007/dsa-2024-322 • https://www.dell.com/support/kbdoc/en-us/000225684/dsa-2024-251 • https://www.dell.com/support/kbdoc/en-us/000221558/dsa-2024-021-idrac-8-and-idrac-9-security-update-for-cve-2023-48795 • https://www.dell.com/support/kbdoc/en-us/000225476/dsa-2024-168-security-update-for-dell-client-bios-for-an-out-of-bounds-write-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225291/dsa-2024-231 • https://www.dell.com/support/kbdoc/en-us/000227795/dsa-2024-342-security-update-for-dell-idrac9-openssh-vulnerability • https://www.dell.com/support/kbdoc/en-us/000228478/dsa-2024-394-security-update-for-dell-avamar-security-update-for-switch-os-10-5-x-gen5a-vulnerabilities

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42772, CVE-2024-21829, CVE-2024-21871, CVE-2024-21781, CVE-2023-43753, CVE-2023-22351, CVE-2023-25546, CVE-2023-41833)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Disclosure of Information and Escalation of Privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL20 Gen10 Plus server - Prior to v3.40_09_06_2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.20_08-07-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v3.40_09_06_2024 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.40_08_01_2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v3.40_09_06_2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.20_08-07-2024 HPE Edgeline e920 Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920d Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920t Server Blade - Prior to v2.20_08-07-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.40_08_01_2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant DL580 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.40_08_01_2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.30_07-31-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.30_07-31-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.30_07-31-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.30_07-31-2024 HPE ProLiant e910 Server Blade - Prior to v3.30_07-31-2024 HPE ProLiant e910t Server Blade - Prior to v3.30_07-31-2024 HPE ProLiant m750 Server Blade - Prior to v3.40_08_01_2024 HPE ProLiant DL60 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL80 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL120 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL160 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL180 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL360 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL380 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL560 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant DL580 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant ML110 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant ML150 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant ML350 Gen9 Server - Prior to v3.40_08-29-2024 HPE Apollo 4200 Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant XL170r Gen9 Server - Prior to v3.40_08-29-2024 HPE ProLiant XL190r Gen9 Server - Prior to v3.40_08-29-2024 HPE Synergy 480 Gen9 Compute Module - Prior to v3.40_08-29-2024 HPE Synergy 620 Gen9 Compute Module - Prior to v3.40_08-29-2024 HPE Synergy 660 Gen9 Compute Module - Prior to v3.40_08-29-2024 HPE Synergy 680 Gen9 Compute Module - Prior to v3.40_08-29-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04699en_us&docLocale=en_US

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.