Advisory Alert

Alert Number: AAA20240923 **Date:** September 23, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Cross-Site Scripting Vulnerability
F5	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Security Update
Description	Dell has released security updates for 20th of September, addressing multiple vulnerabilities that exist in their products. 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/security/en-us/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52846, CVE-2024-26923, CVE-2024-40909)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-52846** - The prp_fill_rct() function can fail. In that situation, it frees the skb and returns NULL. Meanwhile on the success path, it returns the original skb. So it's straight forward to fix bug by using the returned value. **CVE-2024-26923** - Garbage collector does not take into account the risk of embryo getting enqueued during the garbage collection. If such embryo has a peer that carries SCM_RIGHTS, two consecutive passes of scan_children() may see a different set of children. Leading to an incorrectly elevated inflight count, and then a dangling pointer within the gc_inflight_list. **CVE-2024-40909** - After commit 1a80dbcb2dba, bpf_link can be freed by link->ops->dealloc_deferred, but the code still tests and uses link->ops->dealloc afterward, which leads to a use-after-free as reported by syzbot. Actually, one of them should be sufficient, so just call one of them instead of both. Also add a WARN_ON() in case of any problematic implementation. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243350-1/

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2024-20488)
Description	Cisco has released security updates addressing a Cross-Site Scripting Vulnerability that exists in their products. **CVE-2024-20488** - This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Unified CM and Unified CM SME Releases 12.5, 14, 15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-9zmfHyZ

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-34064, CVE-2024-35195)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in Traffix SDC components. **CVE-2024-34064** - The `xmlattr` filter in affected versions of Jinja accepts keys containing non-attribute characters. XML/HTML attributes cannot contain spaces, `/`, `>`, or `=`, as each would then be interpreted as starting a separate attribute. If an application accepts keys as user input, and renders these in pages that other users see as well, an attacker could use this to inject other attributes and perform XSS. **CVE-2024-35195** - HTTP library prior to 2.32.0, when making requests through a Requests `Session`, if the first request is made with `verify=False` to disable cert verification, all subsequent requests to the same host will continue to ignore cert verification regardless of changes to the value of `verify`. This behavior will continue for the lifecycle of the connection in the connection pool. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC version 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000141130 • https://my.f5.com/manage/s/article/K000141129

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.