Advisory Alert

Alert Number: **AAA20230804** **Date:** **August 4, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**Critical**	Authentication Bypass Vulnerability
Ivanti	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
PHP	**High**	Security Update

Description

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2022-1388)
Description	F5 has released a security update addressing an Authentication Bypass vulnerability affecting F5 BIG-IP modules. The vulnerability could allow undisclosed requests to bypass iControl REST authentication. F5 recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	BIG-IP (all modules) 16.1.0 - 16.1.2, 15.1.0 - 15.1.5, 14.1.0 - 14.1.4, 13.1.0 - 13.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K23605346

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-32560, CVE-2023-32561, CVE-2023-32562, CVE-2023-32563, CVE-2023-32564, CVE-2023-32565, CVE-2023-32566)
Description	Ivanti has released a security update addressing multiple vulnerabilities affecting their products. If exploited these vulnerabilities could lead to Stack-based Buffer Overflows, Authentication Bypass and Remote Code Execution. Ivanti recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ivanti Avalanche 6.4 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-Vulnerabilities-Addressed-in-6-4-1?language=en_US

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20593, CVE-2023-2985, CVE-2023-3117, CVE-2023-31248, CVE-2023-3390, CVE-2023-35001, CVE-2023-3812, CVE-2023-3609, CVE-2023-3611.)
Description	Suse has released a security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to Sensitive information disclosure, Denial of Service, Privilege Escalation, Out-Of-Bounds Read/Write. Suse recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4, 15-SP5 Development Tools Module 15-SP4, 15-SP5 Legacy Module 15-SP4, 15-SP5 openSUSE Leap 15.4, 15.5 openSUSE Leap Micro 5.3, 5.4 Public Cloud Module 15-SP4, 15-SP5 SUSE Linux Enterprise Desktop 15 SP4, 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP4, 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233172-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233171-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233182-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233180-1

Affected Product	**PHP**
Severity	**High**
Affected Vulnerability	Security Update
Description	PHP has released a security update addressing multiple vulnerabilities affecting PHP versions prior to 8.1.22 PHP recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	PHP version 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/ChangeLog-8.php#8.1.22

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.