Advisory Alert

Alert Number: AAA20240219 **Date:** February 19, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
F5	**Medium**	Buffer Overflow Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24998 CVE-2022-31159 CVE-2022-30187 CVE-2009-5029 CVE-2010-4051 CVE-2010-4052 CVE-2011-1071 CVE-2011-1089 CVE-2011-1095 CVE-2011-1658 CVE-2011-1659 CVE-2011-2702 CVE-2011-4609 CVE-2011-5320 CVE-2012-3405 CVE-2012-3480 CVE-2012-4412 CVE-2012-4424 CVE-2012-6656 CVE-2013-1914 CVE-2013-2207 CVE-2013-4237 CVE-2013-4332 CVE-2013-4458 CVE-2013-4788 CVE-2013-7424 CVE-2015-0235 CVE-2021-23463 CVE-2021-42392 CVE-2022-23221 CVE-2022-45868 CVE-2022-45688 CVE-2021-31684 CVE-2014-3534 CVE-2014-5077 CVE-2014-5206 CVE-2014-6418 CVE-2014-9940 CVE-2015-8660 CVE-2016-4558 CVE-2016-9777 CVE-2017-1000405 CVE-2017-12146 CVE-2017-17053 CVE-2017-17712 CVE-2017-18202 CVE-2017-6874 CVE-2017-7477 CVE-2018-15471 CVE-2018-18559 CVE-2019-14815 CVE-2019-15917 CVE-2020-12465 CVE-2020-27784 CVE-2020-29369 CVE-2020-35499 CVE-2021-22600 CVE-2021-23133 CVE-2021-29657 CVE-2021-4197 CVE-2022-1651 CVE-2022-1671 CVE-2022-1882 CVE-2022-1943 CVE-2022-1973 CVE-2022-2196 CVE-2022-28796 CVE-2022-28893 CVE-2022-2959 CVE-2022-32250 CVE-2022-3545 CVE-2022-39189 CVE-2022-41222 CVE-2022-4139 CVE-2022-4379 CVE-2022-47518 CVE-2022-47519 CVE-2022-47520 CVE-2022-48424 CVE-2023-0045 CVE-2023-0266 CVE-2023-0386 CVE-2023-0461 CVE-2023-1252 CVE-2023-1390 CVE-2023-1652 CVE-2023-1855 CVE-2023-2006 CVE-2023-2008 CVE-2023-2248 CVE-2023-28464 CVE-2023-28466 CVE-2020-15888 CVE-2006-7250 CVE-2009-0590 CVE-2009-0591 CVE-2009-0789 CVE-2009-1377 CVE-2009-1378 CVE-2009-1387 CVE-2009-2409 CVE-2009-3245 CVE-2009-3555 CVE-2009-4355 CVE-2010-0433 CVE-2010-0740 CVE-2010-0742 CVE-2010-3864 CVE-2010-4180 CVE-2010-4252 CVE-2011-0014 CVE-2011-1473 CVE-2011-1945 CVE-2011-3207 CVE-2011-3210 CVE-2011-4108 CVE-2011-4109 CVE-2011-4576 CVE-2011-4577 CVE-2011-4619 CVE-2012-0027 CVE-2012-0884 CVE-2012-1165 CVE-2012-2110 CVE-2012-2333 CVE-2012-2686 CVE-2013-0166 CVE-2013-0169 CVE-2013-4353 CVE-2013-6449 CVE-2013-6450 CVE-2014-0076 CVE-2014-0160 CVE-2014-3569 CVE-2022-21724 CVE-2022-26520 CVE-2022-31197 CVE-2022-41946 CVE-2021-22060 CVE-2021-22096 CVE-2021-22118 CVE-2015-3414 CVE-2015-3415 CVE-2015-3416 CVE-2015-3717 CVE-2015-5895 CVE-2015-6607 CVE-2016-6153 CVE-2017-10989 CVE-2018-20346 CVE-2018-20505 CVE-2018-20506 CVE-2018-8740 CVE-2019-11811 CVE-2019-16168 CVE-2019-19645 CVE-2019-19646 CVE-2019-8457 CVE-2020-11655 CVE-2020-11656 CVE-2020-13434 CVE-2020-13435 CVE-2020-13630 CVE-2020-13631 CVE-2020-13632 CVE-202)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. An attacker could exploit these vulnerabilities to cause Arbitrary command execution and Brute force attack or a dictionary attack. Dell strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell RecoverPoint for Virtual Machines Versions 5.3 SP2, 5.3 SP2 P1, 5.3 SP2 P2, 5.3 SP2 P4, 5.3 SP3 P1, and 5.3 SP3 P2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222133/dsa-2024-092-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-vulnerabilities

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39340, CVE-2023-41719, CVE-2023-41720)
Description	Ivanti has released security updates addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Denial of Service (DoS), Remote code execution and Privilege escalation. **CVE-2023-39340** - A vulnerability exists on both branches of Ivanti Connect Secure (9.1Rx and 22x) below 22.6R2 or 9.1R18.2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE-2023-41719** - A vulnerability exists on both branches of Ivanti Connect Secure (9.1Rx and 22x) below 22.6R2 or 9.1R18.5 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution. **CVE-2023-41720** - A vulnerability exists on the 22x branch of Ivanti Connect Secure below 22.6R2 where an attacker can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system. Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of Ivanti Connect Secure below 22.6R2 All versions of Ivanti Connect Secure 9.1Rx All versions of Ivanti Connect Secure 9.1Rx below 9.1R18.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-patch-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2023-47038)
Description	F5 has released security updates addressing a Buffer Overflow Vulnerability that exist in the Perl component of F5. The vulnerability is caused when a crafted regular expression is compiled by Perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	F5 BIG-IP Next (all modules) 20.0.1 - 20.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138640

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.