Advisory Alert

Alert Number : AAA20200922 **Date :** September 22, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	**High**	Multiple Vulnerabilities
Samba	**High**	Authentication ByPass
IBM	**High**	Multiple Vulnerabilities

Description

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-8247) (CVE-2020-8246) (CVE-2020-8245)
Description	Multiple vulnerabilities have been discovered in Citrix Application Delivery Controller Citrix Gateway and Citrix SD-WAN WANOP appliance models, **CVE-2020-8245** - Improper Input Validation leads to an HTML Injection attack against the SSL VPN web portal. This will be exploited once an authenticated victim on the SSL VPN web portal opens an attacker-controlled link in his browser. **CVE-2020-8246 –** When an unauthenticated attacker gain access to the management network the Citrix ADC and Citrix Gateway models are vulnerable to a denial of service attack due to uncontrolled resource consumption. **CVE-2020-8247 –** An attacker with escalated privilege due to improper privilege management in Citrix ADC and Citrix Gateway models can be used to execute arbitrary commands on management interface.
Affected Products	Citrix ADC Citrix Gateway Citrix SDWAN WAN-OP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX281474

Affected Product	Samba
Severity	**High**
Affected Vulnerability	Authentication ByPass (CVE-2020-1472)
Description	Netlogon protocol in samba server can be used by an unauthenticated attacker in the network to gain administrative access to the system. This flaw applies to Samba which is used as a domain controller only and Samba file server is not directly affected.
Affected Products	Samba 4.12.6 Samba 4.11.12 Samba 4.10.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2020-1472.html

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-4643, CVE-2020-4590, CVE-2020-14583, CVE-2020-14593, CVE-2020-14621, CVE-2020-14556, CVE-2020-14581, CVE-2020-14579, CVE-2020-14578, CVE-2020-14577, CVE-2019-17639)
Description	IBM has released security patch updates addressing multiple vulnerabilities discovered in IBM WebSphere Application server that is running on AIX, HP-UX,IBM I, Linux, Solaris, windows, z/OS, Mac OS and DB2 running on windows. IBM highly recommends to apply the necessary updates at earliest to avoid system interruptions.
Affected Products	WebSphere Application server (7.0,8.0,8.5,9.0, 17.0.03) DB2 (11.1, 11.2,11.2.1, 12.1, 12.2)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6333623 https://www.ibm.com/support/pages/node/6335335 https://www.ibm.com/support/pages/node/6334311

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.