

March 23, 2020

To: Symantec SiteMinder (previously CA Single Sign-On) Customers

This notice is to alert you to the availability of patches and instructions regarding the Ghostcat vulnerability (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1938> and <https://nvd.nist.gov/vuln/detail/CVE-2020-1938>). This vulnerability is rated at 9.8 Critical Severity. Please give this high attention.

SiteMinder embeds Apache Tomcat in the SiteMinder Access Gateway and the SiteMinder Agent for SharePoint and makes use of the Apache JServ Protocol (AJP). Patches and deployment instructions for the following versions of these SiteMinder components are being made available via this location

<https://techdocs.broadcom.com/us/product-content/recommended-reading/technical-document-index/ca-single-sign-on-hotfix-cumulative-release-index.html#SMWAM>

When you reach that location, search on “Ghost” and you will find a link to deployment instructions and to the patches for each of these:

- Access Gateway (previously SPS) versions 12.8.x, 12.7.x, 12.6.x
- Agent for SharePoint version 12.52 SP1 (all CRs)

The method to exploit this vulnerability is not described in the CVE detail. However, in order to provide a higher level of assurance to our customers we are providing these patches.

If you have questions please contact Broadcom Support:

<https://www.broadcom.com/support/services-support/ca-support/contact-support?intcmp=footernav>