ManageEngine CVE-2022-47966 Vulnerability

https://campus.barracuda.com/doc/98220256/

Severity: 9.8 Critical | RCE | CVSS Attack Vector: Network

Exploit

CVE-2022-47966 is an unauthenticated RCE vulnerability, and it affects Zoho's ManageEngine product portfolio. The vulnerability is a pre-authentication remote code execution (RCE). This CVE is exploitable based on the ManageEngine product and the state of SAML single-sign-on in the current or previous configuration state in certain conditions.

This happens due to the use of Apache "xmlsec" (aka XML Security for Java) 1.4.1. The exploitation is devised based on the vulnerable third-party dependency on Apache Santuario. In some cases, the system will only be vulnerable if SAML-based SSO is currently active.

As a best practice, follow the vendor advisory:
https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

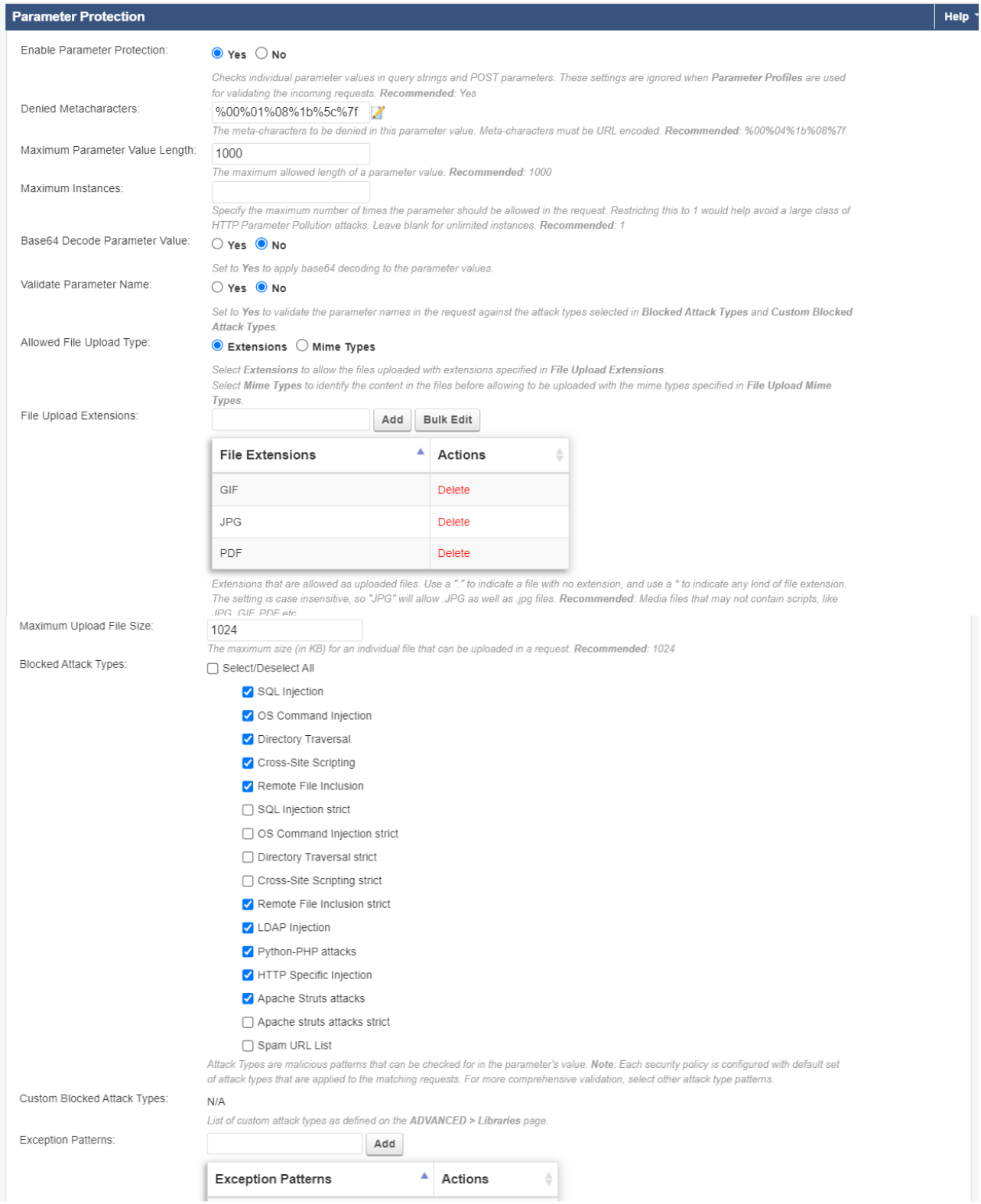
Barracuda WAF Mitigation

The Barracuda Web Application Firewall protects against this attack with the help of the suggested configuration object.

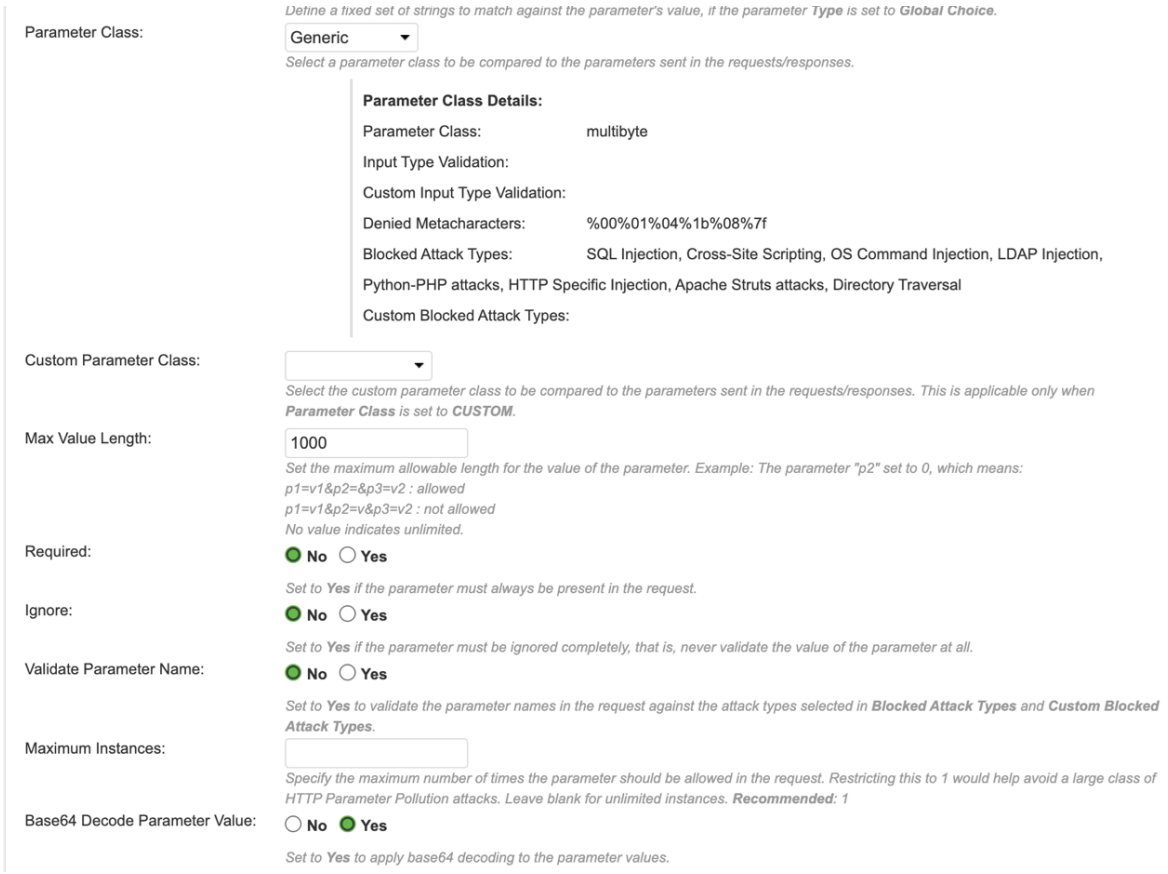
Action Required

1. Ensure **Enable Parameter Protection** is set to *Yes* on the **SECURITY POLICIES > Parameter Protection** page or the **Status** of Parameter Profiles is set to *On* on **WEBSITES > Website Profiles**.
2. Set **Base64 Decode Parameter Value** to *Yes*.
3. Ensure the **Blocked Attack Types** are selected, especially "OS command injection" on the **SECURITY POLICIES > Parameter Protection** page or the appropriate parameter class has the blocked attack types for parameter profiles.

   Parameter Protection:



Parameter Profile:



Related Articles:

- https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
- https://github.com/projectdiscovery/nuclei-templates/pull/6564/files#diff-782cd8c119b60b37026742310fd381c791b4f2e6d2749b4da090e71ea9ba3693
- https://github.com/horizon3ai/CVE-2022-47966

Figures

1. Parameter_Protection.png
2. Parameter Class.png