Globalscape's answers to potential vulnerabilities

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- All products, all versions

DISCUSSION

Over the past decade, EFT has been subjected to a large number of security assessments and pen tests conducted by Globalscape's customers across a wide variety of verticals (banking and finance, government, healthcare, detail, etc.).

The type of security testing employed by Globalscape's customers, along with the tools and techniques used, is often dictated by a combination of the organization's budget and its internal security posture. Based on historical observations, those techniques are typically grouped into the following three categories, from least to most expensive:

1. The organization uses internal IT staff to leverage homegrown or freely available tools to perform manual penetration tests, including fuzzing tools, debuggers, and similar tools.

2. The organization leverages third-application security testing tools such as HP's WebInspect, IBM' AppScan, Tenable's Nessus, Paladion's Plynt, among others.

3. The organization outsources pen testing to a third party, such as ProCheckup, OneConsult, Emaze Networks, A&O Corsaire, SEC Consult, LTI, Cenzic Hailstorm, and many others.

Pen test results of any significance are often shared with Globalscape, typically under NDA. Globalscape has a formal process in place to review potential vulnerabilities, beginning with an in-depth technical assessment by Globalscape's engineering department, which includes categorizing vulnerabilities according to their security impact using CVSS' scoring methodology, followed by a formal technical response that is delivered to our customers detailing whether the vulnerability is a false positive or not, its CVSS score where applicable, any workarounds if available, and the expected fix and remediation timeline.

To date, no active exploit or high CVSS scoring vulnerability has been identified, with most vulnerabilities centered around implementation of best practices, such as applying proper anti-CSRF techniques to EFT's web app pages, using appropriate headers, tagging cookies as HttpOnly, and similar OWASP recommended security techniques. On occasion, a

Globalscape's answers to potential vulnerabilities

vulnerability is reported as a question, such as "How does EFT mitigate against Spectre, Meltdown, or Poodle?" which may result in a fix being deployed, or simply a knowledgebase article that explains how EFT is or is not affected by said situation.

For the current year (2018) the following vulnerabilities were reported:

- A lack of comprehensive support for "no-cache" in addition to the already present "no-store" cache controls
- Questions on whether EFT was affected by Meltdown or Spectre vulnerabilities.
- Concern over CSFR token being communicated over a URL rather than in headers on one of WTC's pages, in accordance with best practices
- A request that EFT provide configurable options so as to only accept a given set of *host headers* to reduce the risk of a host header injection attack (addressed in EFT 7.4.11)

These were minor concerns, with no actual vulnerability or exploit reported, instead mainly consisting of adherence to security best practices.

In addition to customer security testing, which comprises the bulk of EFT's security testing (due to the broad set of tools and techniques used across our customer base), Globalscape conducts its own security testing by using freely available tools provided by HTBridge and Qualsys, applying said scans against each new release of EFT, in particular, its public-facing web client app. Customers can repeat these tests in their own environment by accessing these services directly, as results will varying depending on EFT's configuration. For example, disabling TLS 1.1 in order to force TLS 1.2 will yield a higher score than if TLS 1.1 is left enabled by default.

Through this combination of direct security testing by Globalscape and indirect third-party security testing by our customers, EFT is subjected to an almost constant barrage of tests, which helps us achieve a high level of confidence in the security of our platform. At the same time, we practice "security by design," continually striving to find that perfect balance between optimal flexibility while minimizing attack vectors, so that we can maintain our long-standing reputation as a highly secure yet infinitely flexible MFT platform.

Globalscape's answers to potential vulnerabilities

Any security vulnerabilities found were promptly addressed and included in subsequent patch or major release versions of the software, as captured in the version history. (On the version history page for your product, search for "security.")

Below is a list of Globalscape Knowledgebase articles discussing vulnerabilities addressed in our products.

All products:

11193, Does the GHOST vulnerability affect any Globalscape products

11055, Does GlobalSCAPE release security patches for products separate from general version releases?

EFT:

10589, TCP Sequence Number Approximation Vulnerability

11003, What is GlobalSCAPE's response to the SSL/TLS BEAST exploit?

11050, The server issued one or more cookies that did not have the HttpOnly flag set

11081, Has penetration testing been done against EFT Server?

11096, Is EFT Server vulnerable to the CRIME attack on the SSL protocol?

11173, EFT and SSL Vulnerabilities

11187, The POODLE OpenSSL Vulnerability and Enhanced File Transfer (EFT)

11259, Is EFT affected by CVE-2015-4000 (AKA "Logjam")?

11317, Is EFT vulnerable to SSL vulnerability CVE-2016-6303 (DoS attack)?

11397, Bleichenbacher's ROBOT Vulnerability

Globalscape's answers to potential vulnerabilities

11400, Is EFT affected by the recent “Meltdown” and “Spectre” vulnerabilities?

11448, EFT is NOT affected by the LibSSH vulnerability

11452, EFT Penetration Test Results FAQ

11457, Penetration testing reports indicate that uploading files to EFT is a security risk. How can I prevent that?

11465, XFF and DoS Security Vulnerability

11496, Is my EFT Arcus implementation susceptible to the Azure Stack vulnerabilities?

Mail Express:

11166, The Heartbleed OpenSSL Vulnerability and Mail Express

11186, The POODLE OpenSSL Vulnerability and Mail Express

11261, Mail Express® is NOT vulnerable to the Apache Commons Library exploit

DMZ Gateway:

10646, DMZ Gateway version 3.x uses Java 1.6.0 build 14. Is there any concern over known remote vulnerabilities in this version of Java?

CuteFTP:

11359, Is the HTML editor in CuteFTP affected by the compromised scilexer.dll?

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11446/Globalscapes-answers-to-pote...