Globus Online Security Improvements July 2012

Based on review and feedback from Von Welch [1] and several organizations (XSEDE, PRACE, IGE, …), a number of improvements have been deployed to the production Globus Online system to address all of the critical concerns. These concerns are described here, along with a description for how each was resolved.

1 Address cross site request forgery issues in user interface

Concern: When using the Web or REST interfaces, after authenticating to Globus Online and delegating a credential, a user could visit another site and be tricked (e.g. through a misleading form or a form submitted automatically with JavaScript) into submitting a request back to Globus Online to move data to an unauthorized receiver, or overwrite data from an authorized source.

Resolved: The Globus Online REST APIs (currently Transfer and Nexus) do not accept requests as would be generated by a HTML form element; they only accept AJAX requests. This prevents a form on another site from submitting a request to Globus Online on behalf of a user.

2 Prevent a one time intruder subsequent access from a remote machine

Concern: In the case there is an intrusion to the Globus Online system, the intruder should not be able to obtain anything that allows them to subsequently access protected services from a remote machine.

Resolved: Nexus is Globus Online's data authority for user profiles and related information. It also serves as a credential manager service, facilitating authentication to remote credential services and secure caching of retrieved credentials. Nexus has been updated to use an IP based authentication policy for all privileged client information requests. Currently, access is only allowed from machines running Globus Transfer.

3 Implement state of the art password storage

Concern: Globus Online passwords were not stored salted. If an intruder were able to break in, the user passwords would be susceptible to a rainbow table type attack.

Resolved: Each Globus Online password is now stored with a different salt, a minimum 6 character length, no dictionary words allowed, hashed with a sha512 algorithm, and some additional extra checks.

4 Implement protections against brute force password guessing

Concern: Known brute force password guessing techniques could be used to gain access to user accounts through repeated login attempts.

Resolution: A rate limit algorithm is now used on each password guess. There is a limit of 20 guesses per 10 minutes for each username/source IP pair. That totals to a max of 2880 guesses in a 24 hour period. Guessing a password blindly should take easily millions of guesses. By throttling on username/IP pairs, we avoid the risk of DOS attacks and still make it realistically unfeasible to brute force guess a password.

5 Protect user proxies stored in backups

Concern: Plain text user proxy private keys and certificates could be obtained from backups and if not yet expired, used to access user accounts.

Resolved: Globus Online now encrypts all user proxies stored in backups. Also, Globus Online does not put any private key material on non-ephemeral (EBS) disk.

6 Implement regular firewall or security group testing

Concern: Because the database is a trusting entity, Amazon Security Groups are used to implement a network firewall limiting access to it. Regular monitoring/testing should be implemented to make sure there aren't accidental or malicious configuration changes that expose the database to entities that should not have access.

Resolution: Globus Online's monitoring systems have been enhanced to regularly (hourly) probe the set of ports that are intended to be private. If any of the private ports are found to be open, an alert will be raised. Additionally, monitoring of the production Amazon security group configuration is checked against the last-known-good configuration. If any differences are found, an alert will be raised.

7 Define and document an incident response plan

Concern: For external groups like OSG, XSEDE, NERSC, etc. a defined plan is needed to be prepared when an security incident occurs.

Resolution: Globus Online has written an incident response plan that is available on request. The plan defines a set of procedures that are to be followed if an incident occurs. It was created using the OSG and TeraGrid incident response plans as references.

8 Implement remote logging

Concern: With only local logging on the various Globus Online servers, an intruder can more easily cover their tracks, making it more difficult to determine the extent of actions and changes made during the intrusion.

Resolution: All logins (both application logins and ssh logins) and any access or use of a delegated user credential is logged (append only) to remote server dedicated for just log collection. Access is limited to the security administrators of the Globus Development team.

9 Implement logging for access to user credentials

Concern: User credentials allow Globus Online to access remote machines on a users behalf over a period of time. Any access and use of these credentials should be logged remotely in case of an incident.

Resolution: Any access to a user credential from Nexus or Transfer is now logged.

10 Implement file integrity checking on servers

Concern: File integrity checking helps to ensure that services and configuration changes are readily identified and appropriate steps are taken to validate changes.

Resolution: Globus Online is now using OSSEC to monitor changes to important operating system files and Globus Online specific service files. Maintenance and tuning of the OSSEC rules and alerts will be ongoing.

11 Restrict impact of a stolen delegated proxy

Concern: If an attacker can get hold of a user proxy that has been delegated to the Globus Online service, they could use that proxy to gain shell access to sites that trust that proxy.

Resolution: The XSEDE OAuth MyProxy server has been modified to allow it to be configured to only delegate a limited proxy to Globus Online, which prevents a stolen proxy from being used for GSISSH or GRAM access to a site. In addition, GridFTP has been enhanced to allow a site to configure it to allow access to only certain directories (e.g. home and scratch directories), and to deny access to specified files and directories (e.g., ~/.login, ~/.ssh, etc.).

Reference

1. Von Welch. *Globus Online Security Review*. Indiana University ScholarWORKS, February 2012.