Moore, Jim

From: L. D. Wagoner [ldwagon@super.org]
Sent: Wednesday, July 11, 2007 5:07 PM
To: Moore, Jim
Subject: Updated templates and updated N0073 doc

Attachments: n0072A_relative_path_traversal.html; n0072B_absolute_path_traversal.html; n0072C_UNIX_path_link_problems.html; n0072D_Windows_path_link_problems.html; n0072E_Integer_coercion_errors.html; n0072F_Numeric_truncation_error.html; n0072G_value_problems.html; n0072H_null_pointer_dereference.html; n0072I_race_condition_in_switch.html; n0072J_context_switching_race_condition.html; n0072K_pointer_use_after_free.html; n0072L_memory_leak.html; n0072M_insufficiently_protected_credentials.html; n0072N_privilege_management.html; n0072O_privilege_sandbox_issues.html; n0072P_hard_coded_password.html; n0072Q_expression_issues.html; n0072R_unused_variable.html; n0072S_process_control.html; n0072T_xss.html; n0072U_sql_injection_hibernate.html; n0072V_php_file_inclusion.html; n0072W_stack_overflow.html; n0072X_boundary_beginning_violation.html; n0072Y_wrap_around_error.html; n0072ZA_unsafe_function_call.html; n0072ZB_heap_overflow.html; n0072ZC_equivalent_special_element_injection.html; n0072ZD_os_command_injection.html; n0072ZE_injection.html; n0072ZF_delimiter.html; n0072ZG_server_side_injection.html; n0072ZH_off_by_one_error.html; n0072ZI_sign_extension_error.html; n0072ZJ_common_special_element_manipulations.html; n0072ZK_sensitive_information_uncleared_before_use.html; n0072ZL_discrepancy_information_leak.html; n0072ZM_missing_parameter_error.html; n0072ZN_missing_or_inconsistent_access_control.html; n0072ZO_authention_issues.html; n0072ZP_resource_exhaustion.html; n0072ZQ_unquoted_search_path_or_element.html; n0072ZR_improperly_verified_signature.html; n0072ZS_missing_required_cryptographic_step.html; n0072Z_unchecked_array_indexing.html; n0072ZX_memory_locking.html; N0073.doc







n0072ZK_sensitive_information_... n0072ZL_discrepancy_informatio... n0072ZM_missing_parameter_erro... n0072ZN_missing_or_inconsisten... n0072ZO_authention_issues.html... 0072ZP_resource_exhaustion.ht... n0072ZQ_unquoted_search_path_o...





n0072ZR_improperly_verified_si... n0072ZS_missing_required_crypt... n0072Z_unchecked_array_indexin... n0072ZX_memory_locking.html (7... N0073.doc (591 KB)

Jim,

I updated the N0073 document and associated templates based upon the minutes from the last meeting. I grouped the library function interface weaknesses in the first section of table 8, but left each of the groupings that I had created with their own template until we decide what we're going
to do with them (how we group them, etc.). Four templates (ZT, ZU, ZV, ZW) are no longer needed as they were deemed to be out of scope.

The first section contains:
24, 25, 26, 37, 38, 39, 62, 64, 65, 250, 266, 267, 268: These deal with library functions that interface with a command interpreter and the environment under which the program is executed. One possible solution is providing additional library functions that assist in validating the parameters. We might encourage the development of APIs that provide suitable function.

415 should be treated as a library issue, like the ones mentioned above.

256, 257: Possibly treat as a library issue to provide easy access to crypto techniques and storage cleaning function.

259: This might be a design issue or it might be solved with improved APIs along with 256 and 257.

I also put several of the items in a third section and deemed them out of scope (as based on the minutes):

550, 215: These are design (application) issues and are out of scope of OWGV.

219: This is an application issue and is out of scope.

230: This is a design issue and is out of scope.

446: Design issue. Out of scope.

The remaing ones below need additional discussion. Two in particular, 231/129 and 476/416 on the surface appear to be the same, but are actually quite
distinct and I suggest that we keep them separate.

192, 197: Might be separate; might be combined. Treatment of conversion of integer values.

231, 129: Buffer overflow.

476, 416: Dereferencing pointer containing an invalid value.

365, 368: Race conditions. We had previously decided not to treat concurrency issues in general, but might be willing to support specific cases that occur in the wild, such as these.

401: We're not sure about this one. One could use a language with a garbage collecting memory model and/or explicit storage pools or one

could perform extensive design and code reviews. Are there ways where the library could help? Are there ways in which tooling can help?

591: This seems like a library/API issue. For example, the swap image might be protected in some way.

570, 571,563: We suspect that these are commonly reported by tool vendors as potential problems but are not themselves actual vulnerabilities. On the other hand, these might be a human comprehension issues susceptible to soft guidelines.

Larry