**STANDARD: Potentially Unsafe Code - strlen**

Line: 127 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

|| !strncmp(mg\_get\_request\_info((struct mg\_connection\*)conn)->uri, GRAFANA\_URL, strlen(GRAFANA\_URL))

**STANDARD: Potentially Unsafe Code - strlen**

Line: 128 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

|| !strncmp(mg\_get\_request\_info((struct mg\_connection\*)conn)->uri, POOL\_MEMBERS\_ASSOC\_URL, strlen(POOL\_MEMBERS\_ASSOC\_URL)))

**STANDARD: Potentially Unsafe Code - strlen**

Line: 170 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

mg\_get\_var(qs, strlen(qs == NULL ? "" : qs), name, dst, dst\_len);

**STANDARD: Potentially Unsafe Code - strlen**

Line: 251 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

&& !strncmp(request\_info->uri, GRAFANA\_URL, strlen(GRAFANA\_URL)))

**MEDIUM: Potentially Unsafe Code - strcpy**

Line: 590 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions.

strcpy(referer, r ? r : "/");

**MEDIUM: Potentially Unsafe Code - strcpy(**

Line: 590 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. Can facilitate buffer overflow conditions.

strcpy(referer, r ? r : "/");

**STANDARD: Potentially Unsafe Code - strlen**

Line: 639 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

len = (u\_int)strlen(request\_info->uri);

**STANDARD: Potentially Unsafe Code - strlen**

Line: 810 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

if(strlen(path) > 4 && strncmp(&path[strlen(path) - 4], ".lua", 4))

**STANDARD: Potentially Unsafe Code - (strlen**

Line: 810 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

if(strlen(path) > 4 && strncmp(&path[strlen(path) - 4], ".lua", 4))

**STANDARD: Potentially Unsafe Code - strlen**

Line: 811 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

snprintf(&path[strlen(path)], sizeof(path) - strlen(path) - 1, "%s", (char\*)".lua");

**STANDARD: Potentially Unsafe Code - strlen**

Line: 929 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

snprintf(&ports[strlen(ports)], sizeof(ports) - strlen(ports) - 1, ",%s%s%d",

**STANDARD: Potentially Unsafe Code - strlen**

Line: 950 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

snprintf(&ports[strlen(ports)], sizeof(ports) - strlen(ports) - 1, ",%s%s%d",

**STANDARD: Potentially Unsafe Code - strlen**

Line: 981 - C:\Users\Jeremy\Downloads\HTTPserver.cpp

Function appears in Microsoft's banned function list. For critical applications, particularly applications accepting anonymous Internet connections or unverified input data, strlen and similar functions can become victims of integer overflow or 'wraparound' errors.

http\_prefix\_len = strlen(ntop->getPrefs()->get\_http\_prefix());